5 POLICY AND FINTECH, PART I: FRAMEWORKS

Oliver R. Goodenough, Mark Flood, Matthew Reed, David L. Shrier, Thomas Hardjono, and Alex Pentland

5.1 INTRODUCTION: FINANCIAL INNOVATION AND REGULATORY CONCERNS

Technology has driven innovative changes in many areas of human activity over the past half century, and the financial industry has been no exception. Advances such as the SWIFT system, electronic trading systems, and automated settlement were revolutionary a generation or two ago; now they are business as usual. Aside from the movement toward arm's-length trading fueled by advances in derivatives and securitization, however, the overall structure of the financial system hasn't changed that dramatically. In this way, finance is following a pattern of development common in many industries.

We are moving from a model of technology that empowers human players within the current system to one that replaces many of the human players within the current system, to (inevitably) one where technology overturns much of the current system and replaces it with something else.[1] Much of the innovation already digested in the financial system falls into the first two categories. As the chapters in this book suggest, we are facing developments in finance that begin to look like the third category: something with new and not fully anticipatable outcomes. A series of developments such as blockchain, mobile money, smart instruments, big data, predictive markets, and secure identity are part of the possible revolution.

Among the many uncertainties raised by this vision of disruptive change, regulatory concerns have a significant role. As anyone active in the field knows, the financial system operates within a highly developed set of government rules that can be thought of as the *regulatory framework*. Rules apply to the markets and the transactions within them, to the institutions and to their governance, operations, and net worth, to the nature of currencies, and to the use of data. The list goes on and on. Trying to anticipate the shape of regulatory response, whether prohibitive or enabling, is a key factor in trying to formulate strategies for playing in the world that is dawning.

Against this background, we will explore some of the fundamental policy, regulatory, and governance issues confronting blockchain and related innovations in finance.[2] For the purposes of this chapter, we use the term "regulation" and its variations to encompass a broad range of legal rules, including those made by statute and court decisions as well as those made by regulatory agencies.[3]

Although a full discussion of the implications of fintech is beyond the scope of this chapter, some basic definitions will help orient the discussion. We define *fintech* as any new data- or computation-intensive process or activity that delivers a financial service. Necessity is the mother of invention. Fintech is necessary, because finance, like so many other fields, is confronting a big data revolution, in which the rapidly growing scale of data and information resources overwhelms existing processes.[4] Banny Banerjee argues that one can't fix exponential problems with linear solutions.[5] Fintech is the set of nonlinear new technologies emerging to address the exponential big data challenges. Blockchain and cryptocurrencies are emblematic and high-profile cases, but they do not define the scope of fintech. They merely represent a popular recent use case that has attracted a great deal of attention from private-sector as well as public-sector actors.

We argue that fintech, like any sociotechnical system, will require formal governance mechanisms—including laws and

regulations—to achieve its full potential. The details of these mechanisms should vary, depending on the specific use case under consideration. For example, a digital currency for retail-scale payments will have different needs than a registration system for land titles. This is especially so where currency, unlike land, must travel across jurisdictional borders.

We suggest that regulation has an important, even helpful, role to play in fostering the adoption of fintech.

It is easy to see, for instance, how laws requiring everyone to drive on the same side of the road can speed travel and improve road safety, how standardized weights and measures can facilitate gains in specialization in manufacturing, or how regulations forbidding Ponzi schemes can reduce overall borrowing costs by attracting investors to the market. In contrast to these established examples of productive intervention to solve coordination problems and market failures, fintech is still in its early days. Predicting where its pain points will be most severe or where its successes will be most transformative is necessarily a speculative enterprise.

Regulators and policy makers have increasingly become aware of the need for more sophisticated efforts and greater focus in the area of fintech. Interviews with Commonwealth governments conducted in 2019 by innovation consultancy Visionary Future[6] revealed an array of approaches and levels of sophistication. Twenty governments (primarily their central banks) out of the forty-six Commonwealth central banks were investigated across a range of geographies, country size, and scale of economic development (ranging from the United Kingdom to Trinidad and Tobago). The interviews revealed the following:

- Sixty-five percent of those interviewed had engaged in formal policy development, specifically regarding fintech policy.
- Fifty-nine percent had a fintech policy specialist.
- Only 29 percent had engaged in any form of specialized capacity building regarding fintech.

This clear discrepancy between practice and preparation highlights the importance of documenting effective interventions regarding fintech policy that benefit from appropriate context. The governors of the Commonwealth Central Banks determined that the need for improved practice and expertise was so important that they specifically tasked the Commonwealth Secretariat with developing a policy toolkit and dissemination vehicle.[7]

The discussion that follows is intentionally illustrative rather than exhaustive. We want to show the diversity of challenges that arise in engineering technologically based innovations in our financial system, as well as provide a frame of reference for thinking about those examples. The catalog of possibilities is meant as a starting point. We hope to inspire critical thinking about the issues and approaches to developing fintech, and to encourage stakeholders (government officials, entrepreneurs, ethicists, community activists, developers, and others) to pursue a reasoned approach to regulation.

5.2 REGULATORY GOALS AND TECHNIQUES

5.2.1 Why Do We Regulate?

This section focuses first on why and how regulation happens, highlighting some key guiding principles. It then explores some of the players in the existing regulatory structure governing the financial system. In later sections we apply these principles to blockchain and other fintech innovations. The topic of regulatory design is not a settled one; there are significant arguments and disagreements over where, what, and how regulatory approaches should be applied.[8] That said, there are also some generally recognized guidelines that cut across the debates.[9]

Maximizing the benefits and minimizing the detriments of fintech is not simply a matter of technology. As the economist Paul Romer notes, "Economic growth is driven by the coevolution of two sets of ideas, technologies and rules. Governments

can increase the rate of growth—in ways that benefit all citizens—by creating systems of rules that are both encouraging of and response to innovation; the various goals do not always line up."[10]

To the economist's goal of efficiency we should properly add the lawyer's additional criteria of fairness, justice, predictability, and sustainability.

5.2.2 Jurisdiction

There is a diversity of possible sources of authority in the *making* of rules and also in *applying* them to a particular activity. Who gets to do what is often framed as a question of jurisdiction. What is criminal in one country may be perfectly acceptable in another. Some countries exert *extraterritorial jurisdiction* for some activities, such as the criminal treatment of genocide, but this is relatively rare. More commonly, a country sufficiently concerned about the *effects* of an activity within its borders will assert jurisdiction even if the primary event takes place outside the country. Particularly in the financial markets, where money flows across borders and often to the places of highest yield or safest harbor, countries often affirmatively coordinate common standards of conduct to avoid creating arbitrage opportunities or unfair advantage for one jurisdiction over another. For instance, fraudulent offers are commonly outlawed regardless of the country of origin, and capital adequacy is negotiated to avoid arbitrage.

A further wrinkle on jurisdiction is the ability of the authority in question to get physical control over the person, asset, or other item that is the target of the regulation. This is particularly challenging in the case of cyberactivities, where, for instance, the effects may be felt in the United States but all of the players are in another region of the globe, perhaps one that is antagonistic to US interests. A country may attempt to extend its legal reach, perhaps through extradition, blocking web access, or freezing local accounts, but these measures

often have only limited effect and depend on the goodwill of the other jurisdiction.

Blockchain-enabled activities present particularly interesting jurisdictional challenges because of their inherently dispersed and virtual character. The decentralized and sometimes anonymous nature of blockchain-based transactions is unlikely to remove them from the power of governmental oversight, notwithstanding certain libertarian claims. The internet has posed similar questions, and governments have responded by asserting authority in many contexts. Enforcement of government authority over a dispersed worldwide activity may be a challenge, but as the travails of Silk Road demonstrated, a determined government can overwhelm someone it views as a serious criminal.[11]

5.2.3 Regulatory Goals

What are the proper goals for regulation? Some are cast in negative terms: to prevent harm, both intentional and accidental, whether direct or incidental. Preventing outright predation is usually easy to justify. Innovation, on the other hand, typically harms incumbent interests, and judging when to let such harm proceed is more difficult to assess. The Luddites of eighteenth- and nineteenth-century Britain are often mocked for their opposition to progress, but the negative *local* implications of innovation for wealth and job security may be quite severe (e.g., when the plant closes in a company town), even if the innovation is raising productivity in the aggregate.

Some goals are more positive: to provide an institutional framework within which an activity can grow productively. In this view, the failure to innovate can be seen as causing more harm than the innovation itself. Such a debate is present regarding cryptocurrencies, digital payment systems, and access to banking for the underbanked. Others, such as whether to raise revenue or to consolidate power over an activity, are in the selfish interest of government itself. These

interests can be perfectly legitimate, even when they impose a drag on the activity in question. Less justifiable are examples of *regulatory capture*, where private interests (sometimes intentionally and sometimes unintentionally, such as where information asymmetry produces reliance by the captured) use the power of government to entrench their position in an economic activity. Further complicating the regulatory response to innovation, the various goals do not always line up. Careful regulatory policy often involves balancing competing goods and competing harms so that both the utopian hopes of the innovator and the catastrophic fears of the traditionalist are seldom fully realized. The Clinton-Magaziner e-Commerce Principles shown in box 5.1 provide a case example of a balanced policy intervention that successfully navigated these diverse factors.

Preventing harm The easiest case for legal intervention involves rules against intentional predation, such as physical attack, theft, fraud, and deceit. For example, Bernie Madoff was very properly jailed for willfully defrauding his investors. The Securities and Exchange Commission (SEC) investigates these kinds of activities in the financial markets under its jurisdiction and has recently moved against some particularly questionable promoters of initial coin offerings (ICOs).

Also objectionable is reckless behavior, where the harm per se is not intentional but where any consideration for the prevention of harm is lacking. The failure of underwriters to scrutinize poorly documented subprime mortgages adequately at the point of origination could fall into this category. A third category is harm arising through accidents or unintended systemic effects. A classic example is the bank run, in which the infectious panic of nervous depositors can force even a healthy bank into default.

To justify regulation, a harm need not be inherent in an activity itself, if it is frequently a means to carry out some other harmful action. For instance, a concern sometimes voiced

Box 5.1
The Clinton/Magaziner e-Commerce Principles

The Clinton/Magaziner e-commerce principles, which helped provide a foundation for successful commercial development of internet e-commerce in the United States without sacrificing the public good, are instructive for considering how to regulate other fintech innovations.[12] Briefly, the principles seek to

- maximize the possibility of human freedom because the medium holds great potential to support individual liberty;
- expressly allow voluntary communities to form;
- encourage, where possible, rules set by private, nonprofit, stakeholder-based groups (such as the Internet Engineering Task Force or the W3C Consortium);
- encourage government action that occurs sparingly, transparently, in a targeted manner, and via a common agreement that action is needed;
- respect that internet e-commerce is a decentralized, fast-moving medium, and foster policies that are neutral to specific technologies;
- be global, and therefore an international framework is needed from the outset (rather than the legacy systems where markets evolve locally and then governments coordinate with each other as internationalization occurs).

over virtual currencies is that they can be used to facilitate illicit trafficking in drugs, arms, and people. These secondary effects may cause us to constrain the primary activity.

Providing an institutional framework for private creativity Commercial law provides institutional scaffolding for the design and enforcement of *private* bargains. Contract law is a prime example. At its best, contract law creates a toolkit for designing the enforceable obligations that make specialization and exchange possible, and opens up possibilities for mutual gain.

By making bargains enforceable in *law*, they become much more reliable, and a number of strategic pitfalls can be avoided. On the other hand, contracting between parties with too much disparity in experience or power has risks for deception and predation as well. A good contract framework will discourage fraud by stipulating requirements for disclosure and boundaries of unconscionability.[13] Thus, an appropriate legal scaffolding will *promote* the activity it regulates by solving trust problems that might otherwise hinder adoption. Government intervention to encourage *confidence* in a process is a buttress, not a burden. A familiar example is the oversight of our stock exchanges, where private rules receive public scrutiny under the Securities Exchange Act of 1934.

Much of the interest in blockchain technologies, for example, is that they may be able to help solve these sorts of trust dilemmas. The technology, however, involves relatively arcane cryptographic techniques that can be hard for nonprofessionals to understand and therefore put their trust in them. Moreover, early experiences with fraud in ICOs indicate that a blockchain is not a panacea.[14] A legal framework that helps create confidence that a particular blockchain is properly governed and administered could foster adoption. Box 5.2 reviews a selection of examples that illustrate jurisdictional competition and variation.

Raising public revenue Governments often seek revenues from economic activity, typically through fees or taxes, such as property assessments, customs duties, stamp taxes, value-added assessments, or estate and income taxation. Although the blockchain has libertarian appeal, all competent governments assert the power of taxation broadly. For fintech innovations like the blockchain to evade taxation, they would have to do so in ways analogous to how all illegal activities avoid taxation. Because finance is so information intensive, it is difficult for tax evaders to cover all their digital tracks. At the

Box 5.2
Enabling Rules and Jurisdictional Competition

Each of the fintech innovations discussed in this book raises questions about the current and future adequacy of the legal and regulatory framework to allow its adoption, support its utility, govern its conduct, and resolve disputes.

Adoption of fintech will benefit from adaptations in the code and regulation to foster its growth. This has led to some competition over adopting useful legal infrastructure, as a number of different jurisdictions have sought to attract business. Early movers in the United States include Arizona, Vermont, and Wyoming.

Vermont jumped in early, with a 2015 law setting up a study commission[15] that, in turn, led to a 2016 statute giving evidentiary recognition to records maintained on a blockchain.[16] Subsequent actions have included commissioning a further report on fintech opportunities[17] and, as a result, enacting an enabling provision for a blockchain-based limited liability company (BBLLC).[18] These provisions are aimed at broad support of blockchain activity.[19]

Wyoming has been prolific. In 2018 it set up a blockchain task force that helped promote the adoption of a number of provisions, aimed to a large degree at supporting cryptocurrency initiatives.[20] While undoubtedly useful, this focus is hampered by the SEC's more restrictive posture. At least one SEC commissioner has sought to use a regulatory "safe harbor" to allow public offerings of cryptocurrencies so that they can get to critical circulation levels without running afoul of existing securities laws.[21]

Arizona was the first US jurisdiction to enact a regulatory sandbox for fintech innovation (sandbox approaches are dealt with more extensively in chapter 8 of this volume).[22] This 2018 initiative is under the authority of Arizona's attorney general.[23] As of early 2020 eight companies were participating in the program.[24]

Other states have been active in the past year and are seeking to catch up with these early adopters.

Two states stand out as not being successful with blockchain. In 2016, Delaware, seeking to preserve its leadership

Box 5.2
(continued)

position as the premier state of incorporation, set up the Delaware Blockchain Initiative. In 2017 it passed legislation permitting the use of blockchain as a means of keeping corporate records, including those relating to corporate shares. It began a joint project with a private vendor, Symbiont, with the goal of moving its own public records to blockchain. This all came to a halt, however, with the election of a new governor, John Carney, who was wary of the disruptions this could cause.[25] The state has proceeded at a cautious pace.

In New York, which should be on the forefront of financial innovation, the initial reaction to blockchain was suspicion and tough regulation. In 2015, the state set up the "BitLicense" regime, which requires cryptocurrency businesses to come under licensing and regulation in order to conduct many kinds of transactions. The core provision, set out in 23 NYCRR 200.3(a), is that "No Person shall, without a license obtained from the superintendent . . . , engage in any Virtual Currency Business Activity." In 23 NYCRR 200.2(q), "Virtual Currency Business Activity" is defined as

> the conduct of any one of the following types of activities involving New York or a New York Resident:
>
> receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;
>
> storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
>
> buying and selling Virtual Currency as a customer business; performing Exchange Services as a customer business; or controlling, administering or issuing a Virtual Currency.[26]

Relatively few businesses have sought these licenses, and many have criticized the process as being too restrictive. In December 2019, New York, citing the need to be more open to innovation, proposed amending the approach to provide both greater flexibility and greater guidance for cryptocurrency businesses.[27]

(continued)

Box 5.2
(continued)

There is also competition for innovation at the international level. A number of different jurisdictions have set out to make themselves welcoming to fintech innovation. The United Kingdom, seeking to protect London's powerhouse status as a financial center (notwithstanding the challenges of Brexit), has created a number of opportunities for experimentation, including the most developed fintech sandbox program in the world. First announced in 2015, this initiative of the Financial Conduct Authority is now (2020) in its fifth cohort.[28] Even without this regulatory flexibility, London has been at the center of a fintech boom, with established companies and dozens, if not hundreds, of start-ups working on innovative projects.

Other established financial centers, from Singapore and Switzerland to smaller havens such as Bermuda, Gibraltar, Malta, and the Cayman Islands, have set up initiatives to attract blockchain and other fintech business.

The failure of a financial center jurisdiction to supply the supporting regulatory or legal framework for fintech innovation could encourage the migration of blockchain-based services away from the traditional financial sector and the purview of existing supervisors. There is a long history of jurisdiction shopping by ambitious entrepreneurs, often matched by a "competition in laxity" among eager regulators.[29] The challenge is to prevent support for innovation from devolving into thoughtless permissiveness. Despite the challenge from eager start-ups, however, as yet there has been only limited uptake in friendly jurisdictions that do not already have a thriving financial sector (such as Singapore and the United Kingdom). That said, island nations such as Barbados and Mauritius; US states such as Vermont, Arizona, and Wyoming; and, more recently, the Commonwealth of Nations[30] as an organization have begun developing frameworks to support fintech innovation.

Facebook's Libra is a prime example of this: its creators have argued that the failure of the public sector to provide for a

Box 5.2
(continued)

cross-jurisdictional payment system motivated the entry of this nonfinancial company into the financial sector. This argument is partly self-serving. Cryptocurrencies offer a new avenue for competition in the market for payments services, but incumbent service providers indeed exist for both retail and wholesale cross-border payments. Meanwhile, a payments platform would allow Facebook to integrate purchase and cash-transfer data with its already extensive information on its users.

same time, an open digital ledger facilitates the migration of financial activities, including payments and messages, across borders; in the process, the ledger also potentially exposes the ledger to many legal jurisdictions.

In the United States, the IRS has provided guidance on how to tax cryptocurrency transactions.[31] The basic starting point is that "virtual currency transactions are taxable by law just like transactions in any other property. Taxpayers transacting in virtual currency may have to report those transactions on their tax returns." If you fall under US income tax jurisdiction, there is no legal insulation, because the cryptocurrency asset is virtual.

That said, novel questions may arise when applying the general principles of US taxation to the specifics of cryptocurrency transactions. For instance, in the 2019 Revenue Ruling, the IRS gave guidance on the tax treatment of a "hard fork." It determined that a hard fork in itself did not create a taxable event for a crypto holder, but if the fork was accompanied by an "airdrop" of new tokens, a taxable event would occur.[32]

Protecting existing interests Governments often use their power to protect the economic status quo. This is not always bad; supporting principal providers of goods and services can

benefit both the enterprises and their consumers. In some cases, incumbent providers may be entrenched by the economics of the situation. For example, bitcoin miners appear to be natural monopolies (or at least oligopolies), given that they have converged on a handful of large mining concerns. This is likely due to the large fixed costs of capitalizing the power plant for a mining operation. Similarly, a particular digital currency (e.g., bitcoin versus bitgold) might become a natural monopoly through network externalities. A common public policy response to limit monopoly-power rent seeking is to institutionalize the monopoly as a public utility with democratic governance, like a local water and sewer commission. Some argue that public utility treatment can stifle the emergence of competition that would ameliorate a monopoly situation. Not coincidentally, the bitcoin mine starts to look like a central bank; indeed, central banks, which have extensive experience as governance mechanisms for monetary stability, have taken an active interest in digital currencies.[33]

At the same time, solidification of the status quo can suppress innovation by entrenching both incumbent providers and existing processes. Such suppression can be a by-product of otherwise well-intentioned regulation. Regulators and their charges coevolve over time, and so the incumbent institutions on one side are typically well adapted to the incumbents on the other. Bank examiners know what to expect from well-run banks, and vice versa. The political reality of crisis avoidance is also a powerful force, particularly involving nascent technologies with unclear consequences.

Enshrining one set of interests or market participants over another can have both positive and negative effects. For example, if ex ante rules designed to ensure proper governance, infrastructure, and resilience have the effect of designating (de jure or de facto) a limited, trusted set of miners or other key participants in a distributed ledger structure, confidence in the system and its resilience and potential resolution may

increase. But this same motivation could create a set of unintended consequences such as giving the keys to the system to one set of market participants over another. The result could lead to an undermining of confidence in the system by the very rules designed to bolster that confidence. In any case, policy makers will want to watch how the system evolves with an eye toward facilitating the development of a stable system.

Considerations related to enshrining the interests of one group over another may be necessary for adoption of digital ledger technologies in the financial system, particularly where legal structures have been designed with extant financial intermediaries in mind. For example, derivatives markets are presently subject to a relatively new and comprehensive regime to steer transactions to organized exchanges and central clearing at registered clearinghouses. Centralized markets, such as the Australian Securities Exchange, are already implementing blockchain-based clearing-and-settlement systems to replace legacy infrastructure in their clearinghouses, and entrepreneurs are exploring similar possibilities for over-the-counter markets. If a blockchain technology for clearing and settlement to permit bilateral exchange without the need for centralized trading, clearing, and settlement is widely adopted, changes in law, regulation, and regulatory practice could be required. To avoid regulatory arbitrage, supervisors will need to coordinate, as they have regarding capital requirements for banks or conduct rules for other market participants. Authorities will need to consider how these activities should be governed so that oversight can continue for the protection of the system.

Mitigating wider and secondary effects Regulation should consider both immediate goals and the potential larger effects of an activity. Legal intervention can promote or hinder specific actions, but it can also seek to create systemic effects including efficiency and distributional fairness.

Good rules typically have the goal of helping the users and providers internalize the costs and benefits of an activity. Good

rules also try to avoid unnecessary burden, such as onerous reporting requirements. At the federal level, this principle has been codified in a series of executive orders and OMB Circular A-4 (Office of Management and Budget 2003), which direct the following: "Important goals of regulatory analysis are (1) to establish whether federal regulation is necessary and justified to achieve a social goal and (2) to clarify how to design regulations in the most efficient, least burdensome, and most cost-effective manner."[34]

These principles argue for regulatory restraint. Bitcoin began with the conceit of mimicking a traditional gold standard, which effectively puts its monetary policy on autopilot. Libra's proposal to link to a basket of currencies is reminiscent of the International Monetary Fund's Special Drawing Rights. But cryptocurrencies are gradually learning many of the hard lessons of traditional central banking—for example, that monetary and financial stability are public goods, that both inflation and deflation are important hazards, and that a robust governance framework is critical to a successful monetary system. It is difficult to predict how these forces will evolve, but there is great value in permitting the innovators to experiment, especially at these early stages when the stakes are relatively small.

Rules must also be *socially acceptable*; they must "fit" with cultural norms and conditions. In the United States, traditions of personal autonomy and contractual freedom may make some kinds of otherwise plausible regulatory intervention unacceptable. Indeed, the US income tax system is, in many instances, based on self-reporting, not direct government monitoring of transactions and activities that reflect taxable gains. Thus, for example, even if a blockchain technology could capture income tax revenues through payment systems, it's not clear that society would accept such an intrusion. Likewise, an otherwise efficiency-enhancing rule may be unacceptable because it violates conceptions of "fairness." A

related concept is *cognitive acceptability*. The counterintuitive nature of many economic arguments, such as free trade, monetary expansion, and public expenditure in recessions, makes them hard sells to a public not made up of experts. Given their complicated mathematical and technological basis, blockchain technologies, for example, may suffer similar challenges of understanding.

Another important dimension of innovation is *generativity*, meaning the self-referential modularity that allows some systems to support additional outcomes not envisioned when the system was created. A familiar example of this property is LEGO blocks, which allow the generation, through creative assembly, of a nearly limitless set of shapes. A purpose-built scale-model airplane may be more realistic than the LEGO version, but it cannot be readily converted to anything else. In the domain of rules, the generative nature of the open architecture of the internet is part of its success; no one foresaw Facebook or Uber at the start.[35]

Blockchain technology, developed initially for bitcoin, may also be a generative system, insofar as it enables transformation of existing financial systems in ways not necessarily foreseen. Generativity is also a desirable property for the regulation of innovative technologies—rules should be open to beneficial surprises. That said, there are risks in a generative system. Unanticipated consequences are not always benign, and an open system can be more susceptible to predatory capture. The precautionary principle, which limits the new if there is significant uncertainty around possible harm, would discourage generativity, with its possibility of unintended consequences.[36]

What are the government's concerns for financial regulation? In the case of blockchain, in addition to the general goals to prevent harm and to provide frameworks for growth, there are also concerns for systemic stability. Although one or more government bodies (sometimes federal, sometimes state, sometimes both) generally exist to supervise or regulate

each of these areas, no one body supervises the entire system. Two creations from the 2008 financial crisis—the Office of Financial Research (OFR) and the Financial Stability Oversight Council—do have this system-wide view. Central banks also often take a systemic view—whether authorized by their laws or as an outgrowth of monetary policy responsibilities (the US Federal Reserve has recently started issuing financial stability reports to the public)—and are members, along with several market regulators and coordination bodies (including the US SEC), of the Financial Stability Board in Basel, Switzerland. Through this institutional patchwork, regulators, market watchers, and global coordination bodies have started to focus on the systemic impacts of blockchain-enabled technologies.

The various currently conceived implementations of blockchain in the financial system touch on the basic services noted above (albeit some more than others). In some cases, the migration to blockchain would disrupt little in the financial system and its regulatory framework as currently organized. For example, blockchain as a settlement solution could simply replace current centralized digital ledgers while still residing under the control of a central repository. A number of financial-sector companies have experimented with projects of this kind, but so far most have not resulted in widely adopted services. For instance, Nasdaq joined with other industry partners and piloted a successful margin call system.[37] While there was significant coverage of the pilot, no similar notice has been given of any rollout—at this writing, it appears not to have occurred. A number of these initiatives have involved the firm R3.[38] R3 started out in 2014 as a consortium of large financial institutions seeking to explore blockchain-based applications and has grown into a service provider whose Corda software and platform are powering initiatives for customers across a number of verticals in the financial industry.[39]

On the other hand, blockchain might deeply disrupt other parts of the system, disintermediating existing participants

(perhaps including key players) and raising questions about how crucial monitoring, risk management, and resolution activities might transpire in the context of stress episodes. Steps in this direction are already being taken in insurance contracting and regulation.

In a report issued since the first publication of this chapter, the Financial Stability Board noted, among other things, that fintech can improve financial stability by increasing transparency and through distributed networks dispersing concentration, but it can also accelerate contagion effects and herding, and move risks outside the regulatory perimeter, where the toolkit for dealing with these risks does not exist or has never been applied.[40]

Concerns about distributed ledgers to support cryptocurrencies have become acute in recent months. In the case of Facebook's Libra, the stablecoin would be backed by a basket of fiat currencies—which theoretically limits the possibility of a monetary policy run amok. But monetary policy is notoriously multifaceted and susceptible to unforeseen consequences, and would be even more difficult if it required coordinated national monetary policy efforts to stabilize a coin linked to multiple currencies. Libra's launch raised concerns from all branches of the US government and leaders of both political parties. Fed governor Lael Brainard laid out concerns for Libra that mirrored many of the Financial Stability Board's generalized concerns for fintech: "Liquidity, credit, market or operational risks—alone or in combination—could trigger a loss of confidence and a classic run. . . . The potential for risks and spillovers could be amplified by potential ambiguity surrounding the ability of official authorities to provide oversight and backstop liquidity and to collaborate across borders."[41]

One issue attracting central bankers' attention is nonfinancial "big tech" companies entering into the highly regulated financial world. This is sometimes referred to as "TechFin" because the primary driver isn't the finance piece but the use

of finance to exploit the benefits of the technology piece, like further understanding of customer preferences based on financial transactions or interaction within and with financial markets. While protection of entrenched interests may seem an easy explanation, oversight of banks, brokers, advisers, and other financial intermediaries has fostered transparency and trust and allowed for guardrails that can help contain risks. Recognizing these concerns, Facebook's CEO testified to the US Congress that any Libra system would need regulatory approval or risk abandonment by Facebook itself.[42]

In banking, perhaps more than any other industry, trust is foundational. Deposit insurance, for example, increases that trust. But the government's ability to intervene during a crisis could be challenged if a distributed network doesn't create entry points for the government to intervene in a crisis or simply to adjust monetary policy. Careful system design and governance will be needed. Governments need to intervene in favor of financial stability, to manage risk. The Federal Reserve is monitoring and recalibrating in real time.

5.2.4 Means of Regulating: The Regulatory Toolkit

Traditional systems of regulation and governance often use a relatively well explored "toolkit" of intervention and constraint. These systems can be broadly grouped as those that apply in advance of the activity (ex ante constraints) and those that are applied after the fact (ex post). As fintech innovations such as blockchain or artificial intelligence increasingly underlie a significant portion of our financial transactions, a similarly comprehensive approach can be expected to emerge to govern market players and individual contracts.

The most extreme ex ante intervention is prescription: an outright ban on a particular activity that can be linked to a civil or criminal penalty to give it teeth. This ban can be either a general one or a targeted injunction applied in a particular set of circumstances. Less stringent ex ante approaches include

regulation, qualification, and oversight, often linked to required "best practices." These ex ante governance approaches can especially discourage generative innovation, because they typically set an intentionally constrained framework of possible actions and techniques, with little room for maneuver or discovery.[43] This may be appropriate in high-risk or high-consequence circumstances. Ex ante constraints on behavior also carry strong protections for incumbents, whose processes are typically well adapted to the rules—indeed, incumbents and the rule sets governing them will often coevolve to a comfortable equilibrium. However, if fintech innovations are indeed symptomatic of disrupted traditional processes, we should expect fintech to threaten precisely at points in the system where the entrenched equilibrium is suboptimal.

A softer and more flexible form of ex ante regulation involves ensuring that minimal quality or conduct standards are satisfied either by the individual actor (e.g., TSA prescreening) or by the system (a self-regulatory organization with approved conduct rules, such as a sports league). Registration and licensing can have a beneficial chilling effect on misbehavior by providing a mechanism for excluding players from a profitable game. Registration systems can be designed to retain flexibility of practice but are often linked with established approaches. Membership can require respect for the norms of the club. On the other hand, such systems can act to certify the registrants' reputability to otherwise skeptical users—an example of regulation helping to promote an activity. For example, the National Futures Association, a delegated self-regulatory organization, maintains a registration system to certify firms and individuals for participation. In this case, the industry itself has adopted an ex ante registration mechanism.

Ex post approaches can be more supportive of innovation because they allow activities to proceed, only imposing penalties if the *outcome* is bad. Ex post penalties can be located in the criminal law, often linked to outcomes and not to the

activity itself. Anonymous digital payments are not illegal; anonymous digital payments to support a money laundering syndicate may well be. Similarly, noncriminal consequences can be levied. Whether publicly or privately instigated, these civil penalties can include damages and/or suspension of the activity, either through the removal of a license, through an injunction, or through some other proceeding.

Regulatory regimes often mix and match these ingredients. The SEC requires registration of issuers, exchanges, and broker dealers. There is licensing, and the possibility of delicensing. There are general prohibitions against fraud, with ex post public and private civil remedies and possible criminal penalties. There are specific requirements for disclosure and reporting, and specific practices approved under safe-harbor rules.

Recently, there have been multinational efforts to develop and disseminate best practices in the form of policy toolkits, particularly for banking and finance regulators. Organizations such as the Commonwealth of Nations and the Asian Development Bank (ADB) have explored how the loose coordination of regulatory policy, whether on the axis of shared legal heritage (Commonwealth) or shared regional concerns (ADB), can lead to a more robust environment for business innovation and expansion, on the one hand, and better protection of consumers and more stable financial systems, on the other.

5.2.5 Internal Regulation through the Technology Itself: Code as Law

Regulating an activity that is essentially technological, such as fintech, has the intriguing possibility of building at least some of the desirable practices of that activity into the technology itself. As Lawrence Lessig famously argued regarding the internet, the architecture of a technological system makes rules about what it can and cannot do.[44] In a very real sense, code is law for such purposes.

One reason that a blockchain application like bitcoin or Ethereum has been able to operate with limited legal intervention is that its technical architecture makes it resistant to a wide range of attacks. At the same time, a blockchain can be a component in a larger system with fraudulent or criminal possibilities. There is room for an outside authority to confirm that the architecture does what it purports to do, or to add a layer of societal punishment for those who would try to abuse the service, and perhaps to protect the stability of the system by insisting on mechanisms that produce resilience and confidence. The hacking of the Ethereum system, discussed in chapter 6, illuminates these concerns.

This property of internal regulation creates both a challenge and an opportunity for regulators: Can they participate in the creation of a system to embed good law into the source code itself? Will the designers welcome the presence of regulators? Under what circumstances would the regulators thus expose themselves to liability for any bugs that arise? Would this sort of complicity defeat their effectiveness as enforcers of the rules? There is precedent for such cooperation, but there is also precedent for a more antagonistic relationship that could make such involvement difficult.

There can also be systemic effects of a particular architecture that warrant society's intervention. Individuals acting optimally in their parochial self-interest can cumulatively create misbehaviors that emerge only at the system level, such as bank runs, pricing bubbles, or concentrated risk exposures. Even a blockchain, for example, is not naturally immune to such emergent systemic pathologies.

The exchanges and wallet providers are another point of vulnerability. The chain may be secure, but the points of entry and exit can be corrupted. For instance, in 2013, early in the history of cryptocurrency, bitcoin's Mt. Gox lost over $400 million of bitcoin to hackers, at a time when Mt. Gox

controlled 70 percent of bitcoin trading. In recent years additional theft at these points has occurred. The Selfkey service (admittedly interested) provides a record of hacks. It reports that "$292,665,886 worth of cryptocurrency and 510,000 user logins were stolen from crypto exchanges in 2019."[45] These actors may also rely on outside forces that could (intentionally or not) corrupt their ideals or render them unreliable, such as the exertion of territorial jurisdiction when something of theirs flows through the jurisdiction (e.g., Europe's privacy law, the General Data Protection Regulation) or relies on them (west China's currently cheap source of energy for miners' processors).

Despite the distributed nature of the bitcoin blockchain, market conditions engendered an unhealthy centralization of resources, and bad actors can exploit such weaknesses.

5.2.6 Who Regulates: Federalism, Lawmaking, and Regulatory Agencies

It is worth reviewing where rules originate and how they are enforced. Statutes, enacted by the legislature, are the starting point for most governmentally established regulatory regimes. The United States has a common-law legal system, which means that the legislature shares lawmaking power with courts, which interpret the law to adjudicate specific disputes. This power helps adapt existing legal principles to new circumstances. Thus, even if a statute does not specifically mention a particular fintech application, courts can nonetheless construe existing legal rules to apply to the innovative activity. The backbone of law serves as the authority for flexible and specific rules, either those created by governments or those created by private actors themselves. For instance, the early stock exchanges formed before the regulatory agencies that currently oversee them even existed.

Many regulatory regimes, including most of those related to finance, are assigned for oversight to a regulatory body, such as the SEC or the Federal Reserve. The legislature typically

delegates power to these bodies, allowing them to elaborate specific rules to implement the more general mandates defined in the statutes. This rule-making process is another means for adapting existing governance regimes to fintech applications. Regulators are also frequently the implementation agents for registrations, licensing, inspections, certifications, and other oversight activity, both ex ante and ex post. When civil or criminal laws have been broken, the Justice Department may also help with enforcement.

In the United States the jurisdictions of states and territories also have lawmaking power. Much of the underlying contract and commercial law relevant to fintech is state law. For example, important initiatives at this level include the blockchain enabling law recently adopted in Wyoming and Vermont, and Delaware has launched a blockchain initiative that aims to develop a similarly innovation-friendly legal environment.[46] Where law gets made and enforced is an important element of its possible effects on fintech applications.

5.3 LAWS OF GENERAL APPLICABILITY; CONTRACTS AND INSTRUMENTS

Against this background, we can now examine how law and regulation may apply to future developments in our financial system. Particular fintech innovations will have domain-specific areas of interaction with regulation. They will also often interact with widely shared principles of legal specification.

In this section, we first consider some of the wider principles with the potential for broad application, with particular attention to those affecting financial instruments and contracts. In later sections we will consider more specific use cases of trading markets, identity, and systemic monitoring. Although fintech is applicable to a number of important areas within financial services, these selected examples should help

the reader extrapolate to broader principles of the interaction between regulation and financial technology—particularly in the context of the "why and how" of regulation, discussed above. We reiterate the caution: reading the future is inherently speculative. Some of what we suggest will come to pass; other aspects will not. Our analysis is only a starting point, not a confident road map.

5.3.1 Enabling Legislation I: Existing Provisions

Many financial transactions are constructed around contracts and instruments. These are both creatures of legal recognition, and there are well-developed bodies of law to deal with paper-based examples. In the United States, much of the basic framework on these questions comes from state law. Contracts, property, corporations, and negotiable instruments all depend on laws of states such as New York, California, Massachusetts, or Delaware for their creation as enforceable rules. Financial markets also have a critical overlay of federal rulemaking, such as the US securities, currency, and banking laws and regulations.

In the case of blockchain, its trust-creating nature can substitute for *some* of what law has traditionally done, but we believe that law and regulation will continue to play an important role for blockchain applications. This section will consider examples of legal intervention that will enable blockchain activity by codifying its legal effect. Legal regulation will also aim to accomplish the traditional and linked goals of harm prevention and trust building; this section will examine these as well. In both cases, it will look at existing law and its possible application, along with changes that can be anticipated to deal with concerns specific to a blockchain and its operations.

One question is the degree to which these existing rules may apply to versions created, stored, or even executed via blockchain-enabled digital interaction. A critical existing law is the Uniform Electronic Transactions Act (UETA), promulgated

by the Uniform Law Commission.[47] This 1999 draft law has been adopted, sometimes with some local variation, by most states; notable holdouts include New York and Illinois. UETA provides recognition for transactions recorded and "signed" in digital form, moving beyond paper to authorize digital originals. UETA's prefatory note explains its goals and purpose:

> It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a general contracting statute—the substantive rules of contracts remain unaffected by UETA. Nor is it a digital signature statute. To the extent that a State has a Digital Signature Law, the UETA is designed to support and complement that statute.

While not explicitly aimed at the fintech applications considered here, UETA's scope would cover much of the world of contracts and instruments to be recorded or executed through a blockchain system, including the execution scripts often called "smart contracts." UETA would not necessarily apply to the recording of one-party declarations that lack all the characteristics of a transaction.

In the world of corporations and other business enterprises, some states specifically authorize the bylaws and shares of a corporation, or the operating agreement of a limited liability company, to be expressed in digital originals. For instance, § 2.06 (b) of the Vermont Business Corporations Act provides that the bylaws "may be stored or depicted in any tangible or electronic medium."[48] Vermont and Wyoming are actively updating their laws to enable blockchain activity. More recently, Vermont adopted a subcategory of the limited liability company, the BBLLC, which explicitly addresses issues related to giving a legal framework to blockchain activities. The BBLLC has been used to create the first legally recognized decentralized autonomous organization (DAO) in the United States. Vermont has also enacted a statute to give explicit evidentiary recognition to blockchain recording.

5.3.2 Enabling Legislation II: Provisions That Could Be Added

Enabling provisions, such as those described in the preceding section, may usefully apply to contracts and instruments relying on a blockchain platform, but most such provisions emerged outside of a fintech context. Targeted (fintech-specific) laws are likely to prove useful in unleashing the full potential of fintech for economic commerce and finance. There is widespread use of "tokens" as objects of blockchain commerce. A token can be a strictly *on-chain asset*, like a bitcoin, taking its existence and value entirely as a matter of the operation of the distributed ledger in which it is specified. A token can also be a representation of an *off-chain asset*, such as a parcel of land. This idea is not strictly a new one. For many years, parcels of land have been represented by *deeds*, effectively paper-based tokens. Significant operational problems have emerged in these paper-based title registration systems, but blockchain-based replacements have not been problem-free either.[49] Shares of stock, checks, and the bills of lading used in international trade are other examples of this kind of legacy "tokenization." There are well-developed laws governing paper tokens, but most of them interact with their physical, documentary nature and will fit badly with their digitized descendants.

For instance, the Uniform Commercial Code (UCC) is a widely adopted state-law approach to recognizing and structuring a variety of commercial practices for these legacy tokens, including their use as negotiable instruments. "Negotiability" is the property of an instrument, such as a check or note, intended to be passed from one owner to the next by a process of assignment. Traditionally, this required that the obligation be owed initially to "the order" of a particular person or company. That person, in turn, can make the instrument payable or due to a new holder by endorsement (typically through

signature) and a direction that the instrument is now payable to the order of that new holder. The magic words "to the order of" create this progressive negotiability, until an eventual holder cashes the check, demands payment under the note, or otherwise calls in the underlying bargain contained in the instrument.

A blockchain might manage much of this mechanism of successive token ownership. For instance, ownership transfer of a token representing virtual or actual currency on a blockchain could do much of what a check accomplishes, without needing to involve a bank. Here the blockchain substitutes a somewhat different process for classic negotiation. To get better legal recognition and to avoid a mismatch with existing law, the digital ledger practices would benefit from a specific set of rules in the UCC, either as an amendment to the existing provisions on negotiation or, perhaps more fruitfully, as a new article under the UCC itself.

Smart-contract-based escrow arrangements through a blockchain could also benefit from specific recognition. If you layer a digital triggering mechanism of some kind onto a blockchain currency transfer, you have created something that looks a lot like a traditional escrow agreement. As with negotiation, however, full implementation cries out for a set of rules tailored to the blockchain, and not just borrowed from other contexts with resulting gaps and compromises.

As these examples demonstrate, capturing the potential of blockchain as a vehicle for expressing and executing contracts and instruments will benefit from drafting and enacting well-thought-out enabling provisions. Rather than standing away from traditional law, blockchain proponents should seek to collaborate with law-drafting bodies to develop intelligent solutions that could be enacted broadly in the United States and beyond.

5.3.3 Harm Prevention and Trust Building I: Applications of Current Law

Again, the tasks of building trust in an application and of preventing harm in its use, whether through predation or carelessness, often go hand in hand. The workings of financial markets can be opaque, even to relative experts. Blockchain technology can compound the challenges of opacity. Both trust building and harm prevention can be seen as *credence goods*, which require that users believe in the honesty of providers, without the capacity to monitor them competently.[50] The intervention of a respected regulatory structure can often enhance, rather than impede, markets in credence goods. Much of the regulation of the issuance and trading of financial contracts and instruments targets this domain of harm prevention and trust enhancement. Large portions of this existing regulatory regime should apply to fintech innovations for these purposes.

Fraud—active predation through the use of misleading facts or the suppression of relevant information—is a classic target for preventive regulation in financial markets. The antifraud provisions of the US securities laws are numerous and have wide application. Some are ex ante requirements for filings, disclosures, and approvals for the initial offering and subsequent trading of covered securities. Some are classic ex post punishments for fraudulent activity in the sale or purchase of a security.

The entry-level question is whether the object being traded is a security. This term covers a wide range of financial contracts and instruments, and it can include both blockchain-based and paper-based versions. The *Howey* test usually determines whether something is a security by asking whether "a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."[51] In 2017 the SEC released *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Exchange Act Rel. No. 81207, July 25, 2017). This report warns that cryptocurrency activities could trigger application

of the US securities laws, but it also finds, given the facts and circumstances of this particular case, that the SEC would not bring charges in the case of the DAO and its sale and exchange of DAO tokens. When a cryptocurrency is being organized and marketed by specific promoters and purchased by investors with the expectation of gain from the promoters' efforts, as in the case of many ICOs, the currency is likely to be a security. Once the currency becomes an independent system operating without central control or promotion, it can stop having the characteristics of a security and fall outside the SEC's jurisdiction. An offering might also be exempt if the coins constitute "utility tokens," representing a redeemable right of some kind, like a prepaid drink ticket at a charity event.

In 2017 and 2018 there was a boom in selling new cryptocurrency tokens. According to Cointelegraph (using data supplied by ICObench), 2017 saw 966 ICOs, and in 2018 this number jumped to 2,284.[52] Only a handful of these have attempted compliance with the normal SEC-mandated processes of registration, whether on a full-blown S-1 or via Regulation A. Most either (1) sought out some exemption, such as the broad opening for sales to accredited investors under Rule 506 of Regulation D, (2) claimed *not* to meet the *Howey* test, (3) avoided US jurisdiction on the initial token sales, or (4) just ignored the SEC and plowed ahead. These strategies have met with mixed success.

Early on, the SEC did provide some guidance on whether a particular token was a security, ruling in 2017 that "tokens offered and sold by a 'virtual' organization known as 'The DAO' were securities and therefore subject to the federal securities laws."[53] Staff speeches and actions revealed that established cryptocurrencies, however, such as bitcoin and ether, would probably not be treated as securities.[54]

The SEC introduced an outreach program to help deal with advances in technology. In 2018 it launched a "FinHub" initiative, with the goal of providing "a resource for public

engagement on the SEC's Fintech-related issues and initiatives, such as distributed ledger technology (including digital assets), automated investment advice, digital marketplace financing, and artificial intelligence/machine learning."[55] On May 31, 2019, the FinHub staff hosted a public forum focusing on distributed ledger technology and digital assets, which drew considerable interest.[56] Policy clarity is still a work in progress.

Ironically, for some time the strategy of seeking compliance with the SEC rules was among the least successful. Until 2019, attempts at registration simply stalled in the SEC review process. In July 2019, a request by Blockstack to be allowed to make an ICO under Regulation A+ (effectively an abbreviated approach to a public offering) and under Regulation S to foreign buyers was finally approved after months of regulatory to and fro. The offering closed in November 2019 for a total of $23 million. It remains to be seen whether this really represents a serious thaw in the SEC's willingness to approve cryptocurrency ventures.

The tactic of ignoring the SEC and plowing ahead has been the most dangerous because it may expose promoters to a number of channels for ex post punishment. The most general of these comes under Section 10b of the 1934 Exchange Act and the related Rule 10b-5, which provides the following:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
>
> (a) To employ any device, scheme, or artifice to defraud,
> (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
> (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person,
>
> in connection with the purchase or sale of any security.

To the extent that any of the persons involved in a blockchain-based securities transaction are located in the United States, the blockchain itself would probably count as an "instrumentality of interstate commerce," as would any other technology-based market or transaction platform. This rule creates liability for civil and criminal penalties by the government as well as a civil cause of action for the individuals and businesses harmed by the conduct. There is little doubt that a fraudulent blockchain transaction for securities that met the definitions and jurisdictional requirements of 10b-5 could and would be prosecuted under current law.

Rule 10b-5 is hardly the only law that could apply in the case of blockchain fraud. The general federal law against "wire fraud" (18 U.S. Code §1343) would probably apply (the internet or other vehicle for the chain providing the wire), as well as a number of state antifraud provisions.

As of early 2020, SEC application of its antifraud provisions to ICOs has been spotty. The SEC has charged a few high-profile targets, but all the investigations to date have led to relatively light terms of settlement. For instance, in the 2018 case of the Airfox tokens, sold under the label "AirTokens," the goal was a system for mobile telecommunications companies to offer rewards that customers could redeem in a variety of ways. The ICO raised approximately $15 million, which was intended to establish the technology and business arrangements to support this ecosystem. While purchasers needed to agree that they "were buying AirTokens for their utility as a medium of exchange for mobile airtime," the facts showed that the reality of the transaction was quite different, and that the anticipation of appreciation was an important element in the investor motivation. The agreed remedial actions included a $250,000 fine, registration of the AirTokens as securities under the Exchange Act, together with the reporting involved, and an offer of rescission and repurchase to purchasers of the tokens. No criminal penalties

were assessed; private causes of action by token holders were preserved.[57]

The case of Paragon, described in the same release with Airfox, was similarly decided. Here, the tokens were "ParagonCoins," which would be useful in an ecosystem intended to help the "cannabis community" become more accepted in the mainstream. Elements in this process included providing coworking spaces and various blockchain-based apps to support cannabis sales. The ICO raised approximately $12 million. Although the tokens were to have useful value in exchange for services organized by Paragon, the SEC concluded that the prospect of appreciation was a critical factor in their purchase and sale. The remedial actions were similar: a $250,000 fine, registration of the ParagonCoins as securities under the Exchange Act, together with the requisite reporting, and an offer of rescission and repurchase to purchasers of the tokens. Here, too, no criminal penalties were assessed, and private causes of action by token holders were preserved.

In more recent examples, the SEC in 2019 moved to enjoin sales of tokens being offered by Telegram Group Inc. and its wholly owned subsidiary TON Issuer Inc. The total at stake was reported to be $1.7 billion.[58] And in February 2020, the SEC settled charges against yet another blockchain technology start-up, Enigma MPC, based in San Francisco and Israel. The ICO conducted by Enigma was deemed an unregistered offering of securities. In a now-familiar pattern, Enigma agreed to a claims process that would return funds to its investors, register its tokens as securities, file periodic reports with the SEC, and pay a $500,000 penalty.[59]

How has the SEC been doing? On the one hand, this enforcement has had serious consequences for the enterprises and investors involved; on the other hand, they represent a relatively small slice of the ICO activity that went forward with such ebullience in the cryptocurrency boom. As discussed earlier, one commissioner has suggested that the way to solve this

uncertainty is to provide for a "safe harbor" for ICOs so that they can get to the circulation stage and function as currencies rather than investments.

A further tactic taken under existing securities law approaches involves requiring and certifying structures of private governance. This approach to "self-regulatory organizations" was set up under the Securities Exchange Act of 1934 and originally applied to stock exchanges such as the New York Stock Exchange and to the National Association of Securities Dealers. More recent mergers and reorganizations have led to other organizations such as the Financial Industry Regulatory Authority. The idea is to let the organizations propose and report on their operations and governance rules and regulations, subject to the approval of the SEC. The premise is that the organizations will know their business needs better than a regulator would, and should therefore be the source of the governance approach. Indeed, because many of these self-regulatory organizations are now commercial actors that compete with one another—for example, the market exchanges or central clearing houses—they are incentivized to offer competitive products that are also viewed as safe and fair to the market participants who could choose to do business in a competitor's market. The regulator, on the other hand, can keep an eye out for abusive or otherwise objectionable practices that might find their way into the operations notwithstanding the alignment of interests. Flexibility and generativity are provided for, while still avoiding predation and building trust.

While it has not yet happened, one could imagine the extension of this approach to blockchain providers, with the on-chain structures of process and operation for major tokens that have achieved utility status providing the rules of a self-regulating organization, but still subject to regulatory oversight and review. The Libra Association has conceived something close to this, but oversight of a regulatory organization on a global basis is difficult; and watchers have raised concerns that

the association is nevertheless so tied to Facebook that it lacks real independence and objectivity. One such effort involves the identification of some 1.5 million legal entities through a Global Legal Entity Identifier (LEI) System, managed by a private foundation that adheres to rules laid out and monitored by an informal ("charter based") group of regulators from dozens of countries.

5.3.4 Harm Prevention and Trust Building II: Developing New Law

Existing laws and regulations cannot do the entire job here either. New rules for preventing harm and building trust will be needed to deal with fintech-specific challenges. For instance, the ability to set up automatically executing contracts that cannot be rescinded is sometimes offered as an advantage that fintech could provide. That said, there may be circumstances of fraud or a mistake where it may be necessary to undo a nonrescindable contract. How do you build a "reset button" into a fintech platform and keep the integrity that is a core part of it? Would it involve air gaps (physical separation of computers from network connections) and "ask the human to execute it" moments? What is the legal review and intervention that might be needed to trigger such a circumstance? Contracts frequently contain *severability* clauses, which allow the contract to survive even where a particular offending clause is struck by virtue of a court decision. In such a case, could the code be written to allow the contract to function even without that clause? If not, could the contract be opened to have the rest rewritten so that it operates as newly intended? These questions are explored more fully in section 5.3.6.

As new products emerge, new rules may be needed. We still often envision financial innovations, such as blockchain technology, as better ways of doing things we already understand. We are only just beginning to anticipate the really novel possibilities for setting up and executing agreements and legally

active instruments. Disruptive change is happening, but it is hard to predict in advance. What we can anticipate is that law will be called on to do many of the things it already does to make a new technology trustworthy.

5.3.5 Coordination and Standard Setting

A final area for government activity at a general level is providing mechanisms for coordination and standard setting on the software that can be used to power the platforms and to express the terms of contracts and instruments in executable code. While simply mandating such standards could be attempted, by and large the government seeks to be a catalyst and convener to help private actors agree on common standards. The National Institute for Science and Technology plays such a role, and this kind of activity with respect to the financial markets is part of the mandate of the OFR. Regulatory reporting (financial supervisors' required information collections, in many cases republished for transparency) can itself be a form of standardization. On a global basis, the International Organization for Standardization (ISO) is a private body that develops standards but whose members include governments and whose standards are often baked into official mandates. The LEI, discussed above, adheres to ISO standard 17422, and ISO 20022 covers many financial messaging standards.

A possible step in this direction is the development of a "legal specification language" with the capacity to express and execute the permutations of event and consequence, which are central to many contracts and instruments. Such a language could move blockchain technology, for example, from being a relatively passive ledger for establishing records of transactions to a platform on which their design and execution are carried out. "Smart contracts" and "smart securities" would become quickly computable objects in an ecosystem of like specifications. Elements of this language and system exist; creating the complete package will take not only time and

effort but also the kind of coordination and standard development processes in which government can take an active and useful role.

5.3.6 Techno-legal Aspects of Smart Contracts

The internet technical community has taken an interest in smart contracts, for a number of their promising capabilities. Although smart contracts do not, in general, require a blockchain platform, they are often viewed as an extension of the basic blockchain system found in the bitcoin system. A smart contract today is seen as an *executable code* that is designed to run on specific computing architectures. A given smart contract may be executed on one computer (i.e., one node in the blockchain system), or it may be designed to run concurrently with other related copies of itself, or other smart contracts that are related to (or derived from) itself. The execution of a group of smart contracts may be designed to occur simultaneously, or the contracts may be executed in a cascading or interleaved fashion. These modes of execution may have dramatic ramifications for the outcome of the contract as a unit.

Another dimension of the smart contract paradigm is the fact that multiple parties are typically involved in the actual execution of the contract, including the originator of the smart contract, the computer/node owner or operator where the contract runs, external data sources, and the counterparty in the contract. These various entities need not reside within the same legal jurisdiction.

Today there are a number of open technical issues with regard to smart contracts that may carry legal implications, such as authenticated data sources, correct and complete execution, forensics and postevent evidence, and cross-jurisdiction smart contract executions. All of these are possible targets for the kind of standard-setting activity in which government can play an important role.[60]

NOTES

The views of the authors are their own and not necessarily those of their institutions.

1. O. R. Goodenough, "Legal Technology 3.0," *Huffington Post*, February 4, 2015, http://www.huffingtonpost.com/oliver-r-goodenough/legal-technology-30_b_6603658.html?utm_hp_ref=tw.

2. For convenience, we refer to distributed cryptographic ledgers generically as "blockchain" or "blockchain technology," even though certain variants, such as R3/Corda, don't use blocks.

3. Some discussions of "regulation" limit this term to the more narrow class of rules made by governmental agencies such as the Environmental Protection Agency or the Securities and Exchange Commission (SEC). In this chapter, we use the term in the broader context of governmentally originated rules as described in the text.

4. M. Flood, H. V. Jagadish, and L. Raschid, "Big Data Challenges and Opportunities in Financial Stability Monitoring," Banque de France *Financial Stability Review*, no. 20 (April 2016): 129–142.

5. R. Chase, *Peers Inc: How People and Platforms Are Inventing the Collaborative Economy and Reinventing Capitalism* (New York: PublicAffairs, 2015), 72.

6. Visionary Future, *Commonwealth Fintech Toolkit,* draft report, London, 2019.

7. "Central Bank Heads Keen to Benefit from Fintech Toolkit," Secretariat of the Commonwealth of Nations, 2018, https://thecommonwealth.org/media/news/central-bank-heads-keen-benefit-fintech-toolkit.

8. S. E. Dudley and J. Brito, *Regulation: A Primer*, 2nd ed. (Arlington, VA: Mercatus Center at George Mason University, 2012); R. A. Posner, *A Failure of Capitalism: The Crisis of '08 and the Descent into Depression* (Cambridge, MA: Harvard University Press, 2009); C. R. Sunstein, "Disrupting Voluntary Transactions," in *Markets and Justice: Nomos XXXI*, ed. John W. Chapman and J. Roland Pennock (New York: New York University Press, 1989), 279–302; O. Goodenough, "Governance for Cloud Computing: The Role of Public and Private Rulemaking

in Promoting the Growth of a New Industry" (Vermont Law School Research Paper No. 34-13), http://ssrn.com/abstract=2342594.

9. "Circular A-4," Office of Management and Budget, 2003, https://obamawhitehouse.archives.gov/omb/circulars_a004_a-4/.

10. "Paul Romer," speaker biography, Leigh Bureau, 2012, http://web.archive.org/web/20120606014844/http://www.leighbureau.com/speakers/promer/romer.pdf.

11. A. Greenberg, "Silk Road Creator Ross Ulbricht Sentenced to Life in Prison," *Wired*, May 29, 2015, https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/.

12. I. Magaziner, "Creating a Framework for Global Electronic Commerce," *Future Insight*, Progress and Freedom Foundation, July 1999, http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html.

13. J. A. Drobac and O. R. Goodenough, "Exposing the Myth of Consent," *Indiana Health Law Review*, 2015, http://ssrn.com/abstract=2559341.

14. See S. Shifflett and C. Jones, "Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud," *Wall Street Journal*, May 17, 2018, https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115; S. Dowlat, "Cryptoasset Market Coverage Initiation Network Creation," July 11, 2018, https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ; "Cryptocurrency Anti-Money Laundering Report 2019 Q4," CipherTrace, 2020, https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/.

15. J. Condos, W. H. Sorrel, and S. L. Donegan, *Blockchain Technology: Opportunities and Risks*, Vermont General Assembly, January 15, 2016, https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf; Vermont General Assembly, "The Vermont Statutes Online. Title 12: Court Procedure; Chapter 081: Conduct of Trial,"https://legislature.vermont.gov/statutes/section/12/081/01913.

16. Vermont General Assembly, "An Act Relating to Miscellaneous Economic Development Provisions," bill as passed by the House and Senate, H.868, 2016, https://legislature.vermont.gov/bill/status/2016/H.868.

17. Vermont Law School, *Financial Technology Report*, 2017, https://legislature.vermont.gov/assets/Legislative-Reports/Vermont-Report-Final-Version-December-7.pdf.

18. Vermont General Assembly, "Blockchain-Based Limited Liability Companies," 11 V.S.A. § 4173 et seq., 2018, https://legislature.vermont.gov/statutes/section/11/025/04173.

19. J. Tashea, "Wyoming and Vermont Hope to Attract Tech Entrepreneurs by Passing Laws Favorable to Blockchain," *ABA Journal*, March 1, 2019, https://www.abajournal.com/magazine/article/blockchain-wyoming-vermont-regulations-laws.

20. T. Delahunty, "Wyoming Sets Standard for U.S., Passing 13 Blockchain Laws in 2019," News BTC, 2019, https://www.newsbtc.com/2019/11/20/wyoming-sets-standard-for-u-s-passing-13-blockchain-laws-in-2019/.

21. "Hester Peirce Proposal for Treatment of Cryptocurrency," Anthony L.G., PLLC, March 3, 2020, http://securities-law-blog.com/2020/03/03/hester-peirce-proposal-for-treatment-of-cryptocurrency/.

22. Arizona State Legislature, "Regulatory Sandbox Program," A.R.S. §41-5601 to 41-5612, 2019, https://www.azleg.gov/arsDetail/?title=41.

23. Arizona Attorney General, "Welcome to Arizona's Fintech Sandbox," 2020, https://www.azag.gov/fintech.

24. Arizona Attorney General, "Sandbox Participants," 2020, https://www.azag.gov/fintech/participants.

25. P. Goldstein, "What Is Behind Delaware's New Blockchain Deal with IBM?," State Tech, July 26, 2018, https://statetechmagazine.com/article/2018/07/what-behind-delawares-new-blockchain-deal-ibm.

26. New York State Department of Financial Services, "Virtual Currency Business Activity (BitLicense)," 2020, https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses.

27. New York State Department of Financial Services, "Financial Services Superintendent Linda A. Lacewell Announces New Proposed Regime for Listing Virtual Currencies," press release, December 11, 2019, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1912101.

28. Financial Conduct Authority, "Regulatory Sandbox," 2020, https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

29. Concerns regarding competition in laxity go back at least a century. See E. White, "'To Establish a More Effective Supervision of Banking': How the Birth of the Fed Altered Bank Supervision," in *The Origins, History, and Future of the Federal Reserve: A Return to Jekyll Island*, ed. M. Bordo and W. Roberds (Cambridge: Cambridge University Press, 2011), 7–54; E. Meyer Jr., "Financing Agriculture" (address before the State Bank Division of the American Bankers Association, New York, October 2, 1922), https://archive.org/download/financingagricu00meye/financingagricu00meye.pdf.

30. D. Shrier, "Helping to Level the Playing Field for Regulators—Introducing the Commonwealth Fintech Policy Toolkit," Commonwealth Secretariat, October 7, 2019, https://thecommonwealth.org/media/news/blog-helping-level-playing-field-regulators-introducing-commonwealth-fintech-policy.

31. Internal Revenue Service, "Virtual Currencies," 2020, https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies.

32. Internal Revenue Service, "Rev. Rul. 2019-24," 2019, https://www.irs.gov/pub/irs-drop/rr-19-24.pdf.

33. B. Broadbent, "Central Banks and Digital Currencies" (speech at the London School of Economics, March 2, 2016, Bank of England), https://www.bankofengland.co.uk/speech/2016/central-banks-and-digital-currencies; Bank for International Settlements, *Digital Currencies*, November 2015, http://www.bis.org/cpmi/publ/d137.pdf; European Central Bank and Bank of Japan, *Project Stella: Balancing Confidentiality and Auditability in a Distributed Ledger Environment*, technical report, February 2020, https://www.boj.or.jp/en/announcements/release_2020/rel200212a.htm/.

34. Office of Information and Regulatory Affairs, "Regulatory Impact Analysis: A Primer," 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/regpol/circular-a-4_regulatory-impact-analysis-a-primer.pdf.

35. J. Zittrain, *The Future of the Internet and How to Stop It* (New Haven, CT: Yale University Press, 2008).

36. O. Goodenough, "Generativity: Making Law a More Open Institutional 'Ecosystem' for Productive Innovation" (Vermont Law School Paper No. 4-15, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2589263.

37. M. Huillet, "Nasdaq Blockchain Pilot Handles Margin Calls and Collateral Delivery 'within Minutes,'" Cointelegraph, June 20, 2018, https://cointelegraph.com/news/nasdaq-blockchain-pilot-handles-margin-calls-and-collateral-delivery-within-minutes. See also Nasdaq, "Building on the Blockchain: Nasdaq's Vision of Innovation," 2016, https://www.nasdaq.com/articles/building-blockchain-2016-03-23.

38. R3, "Building the Future of Frictionless Commerce," 2020, https://www.r3.com/wp-content/uploads/2020/02/R3_Corporate_Brochure_Letter_Digital_feb_2020.pdf.

39. R3, "Customers," 2020, https://www.r3.com/customers/ works.

40. Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention*, June 27, 2017, https://www.fsb.org/wp-content/uploads/R270617.pdf.

41. L. Brainard, "Digital Currencies, Stablecoins, and the Evolving Payments Landscape," October 16, 2019, https://www.federalreserve.gov/newsevents/speech/brainard20191016a.htm.

42. U.S. House Financial Services Committee, "An Examination of Facebook and Its Impact on the Financial Services and Housing Sectors," Hearing Memorandum, October 23, 2019, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=404487.

43. L. Kaplow, "Rules versus Standards: An Economic Analysis," *Duke Law Journal* 42 (1992): 557–629, http://scholarship.law.duke.edu/dlj/vol42/iss3/2.

44. L. Lessig, "Codev2," 2005, http://codev2.cc/download+remix/Lessig-Codev2.pdf.

45. Selfkey, "A Comprehensive List of Cryptocurrency Exchange Hacks," February 13, 2020, https://selfkey.org/list-of-cryptocurrency-exchange-hacks/.

46. Delaware Office of the Governor, "Governor Markell Launches Delaware Blockchain Initiative," *PR Newswire*, May 2, 2016, http://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html.

47. Uniform Law Commission, "Uniform Electronic Transactions Act (1999)," National Conference of Commissioners on Uniform State Laws, 1999, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=2c38eebd-69af-aafc-ddc3-b3d292bf805a.

48. Vermont General Assembly, "Vermont Business Corporations: Incorporation: Bylaws," 11A V.S.A. § 2.06, 2010, http://legislature.vermont.gov/statutes/section/11A/002/00002.06.

49. On the challenges of paper-based title registration, see J. P. Hunt, R. Stanton, and N. Wallace, "US Residential-Mortgage Transfer Systems: A Data-Management Crisis," in *Handbook of Financial Data and Risk Information*, vol. 2, *Software and Data*, ed. M. Brose, M. Flood, D. Krishna, and W. Nichols (Cambridge: Cambridge University Press, 2014), 85–132. On blockchain-based alternatives, see V. L. Lemieux, "Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective," *European Property Law Journal* 6, no. 3 (December 2017): 392–440, https://doi.org/10.1515/eplj-2017-0019.

50. A. Wolinsky, "Competition in Markets for Credence Goods," *Journal of Institutional Theoretical Economics* 151 (1995): 117–131.

51. SEC v. W. J. Howey Co., 328 U.S. 293 (1946), 299, https://scholar.google.co.uk/scholar_case?case=12975052269830471754&q=SEC+v.+W.+J.+Howey+Co.,+328+U.S.+293+(1946)&hl=en&as_sdt=2006&as_vis=1.

52. D. Pozzi, "ICO Market 2018 vs 2017: Trends, Capitalization, Localization, Industries, Success Rate," Cointelegraph, January 5, 2019, https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate.

53. Securities and Exchange Commission, "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities," press release, July 25, 2017, https://www.sec.gov/news/press-release/2017-131.

54. B. Pisani, "Bitcoin and Ether Are Not Securities, but Some Initial Coin Offerings May Be, SEC Official Says," CNBC, June 4, 2018, https://www.cnbc.com/2018/06/14/bitcoin-and-ethereum-are-not-securities-but-some-cryptocurrencies-may-be-sec-official-says.html; Securities and Exchange Commission to Jacob E. Comer, re: Cipher Technologies Bitcoin Fund, October 1, 2019, https://www.sec.gov/Archives/edgar/data/1776589/99999999719007180/filename1.pdf.

55. Securities and Exchange Commission, "SEC Launches New Strategic Hub for Innovation and Financial Technology," press release, October 18, 2018, https://www.sec.gov/news/press-release/2018-240.

56. Securities and Exchange Commission, "SEC Staff Announces Agenda for May 31 Fintech Forum," press release, April 24, 2019, https://www.sec.gov/news/press-release/2019-59.

57. Securities and Exchange Commission, "Two ICO Issuers Settle SEC Registration Charges, Agree to Register Tokens as Securities," press release, November 16, 2018, https://www.sec.gov/news/press-release/2018-264.

58. Securities and Exchange Commission, "SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering," press release, October 11, 2019, https://www.sec.gov/news/press-release/2019-212.

59. Securities and Exchange Commission, "ICO Issuer Settles SEC Registration Charges, Agrees to Return Funds and Register Tokens as Securities," press release, February 19, 2020, https://www.sec.gov/news/press-release/2020-37.

60. A detailed discussion of these elements is beyond the scope of this chapter. We may address them in a future document.