Humans Judged by Machines: The Rise of Artificial Intelligence in Finance, Insurance, and Real Estate

Frank Pasquale

Contents

Introduction	119
Incrementalist Fintech: The Problems of Predatory, Creepy, and Subordinating Inclusion	120
Fallacies of Futurist Fintech	122
References	126

Abstract

There are opportunities but also worrisome trends as AI is applied in finance, insurance, and real estate. In these domains, persons are increasingly assessed and judged by machines. The financial technology (Fintech) landscape ranges from automation of office procedures, to new approaches for storing and transferring value, to the granting of credit. The Fintech landscape can be separated into “incrementalist Fintech” and “futurist Fintech.” Incrementalist Fintech uses data, algorithms, and software to complement professionals who perform traditional tasks of existing financial institutions. It promises financial inclusion, but this inclusion can be predatory, creepy, and subordinating. These forms of financial inclusion undermine their solvency, dignity, and political power of borrowers. Futurist Fintech’s promoters claim to be more equitable, but are likely to falter in their aspiration to substitute technology

for key financial institutions. When used to circumvent or co-opt state monetary authorities, both incrementalist and futurist Fintech expose deep problems at the core of the contemporary digitization of finance.

Keywords

Artificial intelligence · Finance · Insurance · Real estate · Fintech · Privacy · Employment

Introduction

The financial technology (“fintech”) landscape is complex and diverse. Fintech ranges from automation of office procedures once performed by workers, to some genuinely new approaches to storing and transferring value, and granting credit. Established and start-up firms are using emerging data sources and algorithms to assess credit risk. And even as financial institutions are adopting some distributed ledger technologies, some proponents of cryptocurrency claim that it “changes everything” and will lead to a “blockchain revolution.”

For purposes of this paper, I will divide the fintech landscape into two spheres. One, incrementalist fintech, uses new data, algorithms, and software to perform classic work

I wish to thank the organizers of the 2019 PAS/PASS Workshop on AI and robotics for giving me the opportunity to present this work. I also wish to thank Raymond Ku, and the audience at Case Western Reserve University, for thoughtful comments on this work when it was presented as the 2019 Center for Cyberspace Law and Policy Distinguished Lecture. This work is planned to be simultaneously published in the Case Western Reserve University Law Review.

F. Pasquale (✉)
Brooklyn Law School, Brooklyn, NY, USA
e-mail: pasquale.frank@gmail.com

of existing financial institutions. This new technology does not change the underlying nature of underwriting, payment processing, lending, or other functions of the financial sector. Regulators should, accordingly, assure that long-standing principles of financial regulation persist here. I address these issues in Part I below.

Another sector, which I deem “futurist fintech,” claims to disrupt financial markets in ways that supersede regulation, or render it obsolete. For example, if you truly believe a blockchain memorializing transactions is “immutable,” you may not see the need for regulatory interventions to promote security to stop malicious hacking or modification of records. In my view, futurist fintech faces fundamental barriers to widespread realization and dissemination. I address these issues in Part II below.

Incrementalist Fintech: The Problems of Predatory, Creepy, and Subordinating Inclusion

Over the past decade, algorithmic accountability has become an important concern for social scientists, computer scientists, journalists, and lawyers. Exposés have sparked vibrant [debates](#) about algorithmic sentencing (van Dam 2019). Researchers have exposed tech giants [showing](#) women ads for lower-paying jobs, [discriminating](#) against the aged, deploying deceptive [dark patterns](#) to trick consumers into buying things, and manipulating users toward rabbit holes of extremist content (Gibbs 2015; Angwin et al. 2017; Warner 2019). Public-spirited regulators have begun to address algorithmic transparency and online fairness, building on the work of legal scholars who have called for technological [due process](#), platform [neutrality](#), and nondiscrimination [principles](#) (Citron 2008; Pasquale 2008, 2016).

Establishment voices have hailed fintech as a revolutionary way to include more individuals in the financial system. Some fintech advocates advocate radical deregulation of their services, to enable their rapid entry into traditional banking markets. However, there is a risk of the fintech label merely masking “old wine in new bottles.” The annals of financial innovation are long, but not entirely hallowed (FCIC 2011). When deregulatory measures accelerated in the late 1990s and early 2000s, their advocates argued that new technology would expertly spread and diversify risk. However, given biases in credit scores based on “fringe” or “alternative” data (such as social media use), even the finreg (finance regulatory) establishment is relatively comfortable with some basic anti-bias [interventions](#) (Scism 2019).

New quantitative approaches to underwriting and reputation creation have often failed to perform as billed, or

have raised serious normative concerns¹ (Pasquale 2015). Most fundamentally, a technology is only one part of a broader ecosystem of financial intermediation (Lin 2014, 2015²). AI underwriting may feed into a broader culture of total surveillance, which severely undermines human dignity. Regulators must ask larger questions about when “financial inclusion” can be [predatory](#), creepy (as in [24/7 surveillance](#)), or subordinating (as in at least one Indian fintech app, which [reduces the scores](#) of those who are engaged in political activity) (Hill and Kozup 2007; Taylor 2019; Variyar and Vignesh 2017; Vincent 2015).

Limiting the factors feeding into credit decisions is important, because our current path is toward a “full disclosure future.” For some fintech firms, everything is fair game. Each week brings new examples of invasive data collection. Before they push consumers to accept even more Faustian bargains for better credit terms, regulators need to decide how far data collection can go.³ According to one aggrieved worker, her boss “bragged that he knew how fast she was driving at specific moments ever since she had installed the app on her phone” (Vincent 2015). Progressive car insurance offers discounts for car tracking devices that measure “hard stops,” among other putative indicators of bad driving.

Nor is this kind of tracking simply a matter of consumer choice. Once enough people agree to a certain kind of tracking, refusing it looks suspicious. What have you got to hide? (Peppet 2015). Moreover, in a market economy, no firm wants to risk falling behind others by lacking data they have. The insurer John Hancock gave us an early glimpse of how the ensuing dynamic plays out. It sells life insurance to those who will wear FitBits, Apple Watches, or similar devices (The Guardian Editorial 2018; Senior 2018; Barlyn 2018). Life insurers also want to scour applicants’ social media accounts, to spot “red flags” for dangerous behavior (Scism 2019).

We all may be emitting other “tells” that are more grave. For instance, researchers recently parsed the mouse movements of persons who extensively searched for information about Parkinson’s disease on Bing (White et al. 2018). This group—which is far more likely to have Parkinson’s than the population as a whole—tended to have certain tremors in their mouse movements distinct from other searchers. These tremors were undetectable by humans—only computers can clock the microseconds difference in speed that distinguished normal from pathological tremors. Thus, there is no defense

¹Pasquale (2015) describes search results as a form of reputation creation (for name searches) that can create serious normative and ethical concerns.

²Lin (2014, 2015) offer 10 regulatory principles for the new financial industry.

³For an overview of the issues raised, see Bruckner (2018).

to such detection—no “privacy enhancing technology” that can prevent such technology, once developed, from classifying someone as “likely to develop Parkinson’s.” The more data about troubling fates is available, better AI will get at predicting them. We may want our doctors to access such information, but we need not let banks, employers, or others use it.

All of the scenarios explored above have been hailed as part of a tsunami of data-driven “financial inclusion.” True, if financial firms have access to more information about potential clients, some persons who once would not have been part of the financial system will likely gain access to credit. But there is more to life—and public policy—than consenting transactions among persons and fintechs. Without proper guardrails, there will be a race to the bottom in both sharing and behavior shaping, as more individuals compete for better deals. That would result in a boom in predatory inclusion (which harms more than it helps), creepy inclusion (which gives corporate entities a voyeuristically intimate look at our lives), and subordinating inclusion (which entrenches inequality by forcing people to maintain the same patterns of life that resulted in their desperation in the first place). Lawmakers should discourage or ban each of these types of “inclusion.”

Predatory inclusion is a concept with a long history (Seamster and Charron-Chénier 2017). Credit enables, while its shadow side (debt) constrains. When those desperate for opportunity take on a heavy loan burden to attend training programs of dubious value, the latter effect predominates. The rhetoric of uplift convinces too many that more learning is a sure path to better earning power. Fly-by-night, for-profit colleges take advantage of their hope (McMillan Cottom 2018). They peddle a cruel optimism—that the future has to be better than the past (Berlant 2011; Blacker 2013; McGettigan 2013; Newfield 2016).

The same principle also applies to “creepy inclusion.” AI (and the data collection it is now sparking) allows lenders to better microtarget vulnerable consumers (Upturn 2015; Mierzewski and Chest 2013). A sophisticated firm might notice a parent in December rapidly re-ordering toy options by price, and may track their phone as they walk from store to store without buying a child’s present. “Vulnerability-based marketing” may even enable the ad to be timed, at the very point in the day when despair is most likely to set in. A bright blinking message “Let our credit save your Christmas!” may be well-nigh irresistible for many strapped parents. This vulnerability-based marketing will only get worse with the spread of 24/7 tracking hypothesized above. This is one reason I would call the offer of better credit terms in exchange for nonstop cell phone tracking, archiving, and data resale a prime example of “creepy inclusion.” (Kotsko 2015; Tene and Polonetsky 2014).

If a boss asked an employee if she would mind him trailing her twenty-four hours a day, seven days a week, the feeling of threat would be imminent. She might even be able to get a restraining order against him as a stalker. A cell phone tracker may seem like less of a threat. However, the use and re-use of data creates distinctive and still troubling menace. Creepiness is an intuition of future threat, based on a deviation from the normal. Normal experience is one of a work life distinct from home life, and of judgments about us being made on the basis of articulable criteria. Creepy inclusion disturbs that balance, letting unknown mechanical decision makers sneak into our cars, bedrooms, and bathrooms.

Of course, at this point such surveillance demands are rare. Financial sector entrepreneurs brush aside calls for regulation, reassuring authorities that their software does not record or evaluate sensitive data like location, person called, or the contents of conversations.⁴ However, metadata is endless, and as seen with the example of the hand tremors predicting Parkinson’s, can yield unexpected insights about a person (ACLU 2014). Moreover, now is the time to stop creepy inclusion, before manipulative marketing tricks so many people into bad bargains that industry can facilely assert its exploitation is a well-established “consumer preference.”

The timing issue is critical, because industry tries to deflect regulation when a practice first begins, by saying that it is an “innovation.” “Wait and see how it turns out,” lobbyists say. But once a practice has been around for a while, another rationale for non-regulation emerges: “How dare you interfere with consumer choice!” This cynical pair of rationales for laissez-faire is particularly dangerous in data regulation, since norms can change quickly as persons jostle for advantage (Ajunwa et al. 2017). Uncoordinated, we can rapidly reach an equilibrium which benefits no one. Cooperating to put together some enforceable rules, we can protect ourselves from a boundless surveillance capitalism (Zuboff 2019). For example, some jurisdictions are beginning to pass laws against firms “microchipping” workers by subcutaneously injecting a rice-sized sensor underneath their skin (Polk 2019).⁵ Others are beginning to require operators of AI and bots to disclose their identity (Pasquale 2017).

That project of self-protection is urgent, because “subordinating inclusion” is bound to become more popular over

⁴For an example of this kind of distinction, note the assurances from one such firm in Leber (2016).

⁵Some “supporters argue that these are ill-informed concerns, easily addressed with information about the safety of the devices, and how they will and will not be used. They contend that chipping is really no different than having employees carry around electronic access cards that are used for entry into buildings and purchases at the company cafeteria, but with significant advantages of convenience and security because employees can’t forget their chip, lose it, or have it stolen.” (Polk 2019). However, an access card is not injected into a person’s body. The potential for a “Stockholm Syndrome,” or what Sacasas calls the “Borg Complex,” is strong. See, e.g., Metz (2018), Sacasas (2013).

time. Penalizing persons for becoming politically involved—as firms in both India and China now do—further entrenches the dominance of those who provide credit over those in need of it. The rise of what some call “vox populi risk (Citi 2018)”—including the supposed “danger” of persons demanding corporations treat them better—will provoke more executives to consider the political dimensions of their lending. Firms may well discover that those who get involved in politics, or sue their landlords for breach of a lease, or file a grievance at work, are more likely to contest disputed charges, or are even more likely to default. But such correlations cannot inform a humane credit system. They set us all on a contest of self-abasement, eager to prove ourselves the type of person who will accept any indignity in order to get ahead.

While predatory, creepy, and subordinating inclusion are objectionable on diverse grounds, they all clarify a key problem of automation. They allow persons to compete for advantage in financial markets in ways that undermine their financial health, dignity, and political power. It is critical to stop this arms race of surveillance now, because it has so many self-reinforcing internal logics.

Fallacies of Futurist Fintech

Though sober reports from the World Economic Forum (2017), Deloitte, and governmental entities accurately convey the problems and opportunities posed by the incrementalist side of fintech, much of the excitement about the topic of financial technology arises out of a more futuristic perspective. On Twitter, hashtags like #legaltech, #regtech, #insurtech, and #fintech often convene enthusiasts who aspire to revolutionize the financial landscape—or at least to make a good deal of money disrupting existing “trust institutions” (e.g., the intermediaries which help store and transfer financial assets).

Finance futurism fits with broader industry narratives about the role of automation in transforming society. Captains of finance capital have long aspired to automate work. Machines don’t demand raises or vacations. They deliver steady returns—particularly when protected by intellectual property law, which may forbid competitors from entering the market. The “dark factory”—so bereft of human workers that not even lights are needed in it—is a rentier’s dream. Finance has long demanded that factories increase their productivity via better machinery; now it has turned the tools of automation on itself. An upper echelon of managers and traders has displaced analysts, accountants, and attorneys with software. Ordinary investors fleeing fees are opting for “set-it-and-forget-it” index funds, which automatically allocate money to a set list of stocks and bonds. “Robo-advisers” present such options via low-key, low-pressure apps. Bots exchange buy and sell orders. Boards are con-

stantly pressuring management to push “AI” further up the value chain, replacing managerial judgment with machine learning. Finance’s self-automation is a familiar ideological story of capitalism: one of market competition pushing firms and entrepreneurs to do more with less.

With the rise of cryptocurrency, another ideology—a mix of anarcho-capitalism and cyberlibertarianism—is strengthening this regnant neoliberal model of automation. Imagine distributed software that allowed you (and those you transact with) to opt out of using banks altogether. When you buy something online, a distributed ledger would automatically debit your account—and credit the seller’s—with the exact amount of the purchase, recorded in *all* computers connected to the network, so that tampering with the common record was effectively impossible. Now imagine that humble arrangement scaled up to the sale and purchase of equities, bonds—almost anything. Fees on investing might fall below even 0.1%—just enough to keep the distributed ledger maintained and updated. If the ledger itself could automatically “pay” those who do its work with tokens valued as money, perhaps fees could drop to zero.

The system just described is starting to develop. Bitcoin and other cryptocurrencies function as the tokens described above, while blockchains serve as the distributed ledgers. However, its implications are far from clear. Users opt out of traditional finance for a reason, and simply avoiding wire transfer fees does not seem like a plausible rationale for taking on the risks of the new. Using crypto to evade regulation, sweetens the pot. Critics fear these new “coins” are primarily a way to grease the skids of a pirate economy of data thieves, money launderers, and drug dealers (Beedham 2019). The cyberlibertarian rejoinder is a simple one: people deserve to do what they please with their assets—tax authorities, court judgments, or financial regulators be damned.

Finn Brunton’s *Digital Cash* entertainingly narrates the stories of *soi-disant* renegades who aspired to set up their own systems of currency to operate independently from extant legal systems (Brunton 2019). On the one hand, these would-be prophets of monetary systems beyond or beside or hidden from the state, aspire to exist outside the system, ostensibly because of their disgust with crony capitalism and all its trappings. On the other, as soon as some of their schemes get sufficient traction, there is a scramble to convert the “anti-system” digital assets of pioneering cryptocurrency promoters into safer, more familiar equities, bonds, and interest-bearing bank accounts.

Brunton offers a “history of how data was literally and metaphorically *monetized*,” as promoters of digital cash tried to make digital data *about stores of value* itself valuable (Brunton 2019, p. 3). This bootstrapping is reminiscent of the history of fiat money itself, which arose in part to pay tributes, taxes, and fees imposed by the state. We can think of the distributed ledger I described above as data—a representation

of who has what: of who owes, and who owns. Bitcoins originate as ways of rewarding those who expended the computational power necessary to maintain the ledger. What can make Bitcoins so authoritative, so valuable, that persons have gladly traded 18,000 U.S. dollars for one of them?

The answer is narrative: the stories we (and our friends, the media, and our social media feeds) tell ourselves about how value is created and stored. As Brunton argues, “the history of digital cash can also show us a particularly vivid example of the use of money and technologies to tell stories about the future.” (Brunton 2019, p. 3). Nobel Prize winning economist Robert J. Shiller has recently highlighted the importance of “narrative economics” for understanding why certain conceptions (and misconceptions) of commercial life come to dominate the thought of policymakers, politicians, and people generally (Schiller 2019). One critical narrative step toward cryptocurrency is a negative one: widespread acceptance of tales of distrust and disillusionment at the existing financial order. These were not hard to find in the wake of the Global Financial Crisis (GFC) of 2008. Scores of books chronicled self-dealing in leading financial firms, and questioned the wisdom of government interventions. Bitcoin was announced in late October 2008, and the first entry in its ledger (the so-called “genesis block”) included a reference to bank bailouts.

Brunton elegantly recounts a primordial stew of ideas that encouraged crypto enthusiasts in the decades leading up to Bitcoin, when alternative currencies were rare and isolated. He describes isolated “agorists,” who saw every transaction between individuals without state-sponsored money as a victory for private initiative over public control (Brunton 2019, p. 3). Some were inspired by J. Neil Schulman’s 1979 novel *Alongside Night* (set in a dystopian 1999 New York beset by hyperinflation), where “characters move to or inhabit alternative zones, where they can live outside the emergency, exacerbate the existing crisis, and return to the changed world on the other side of the disaster where their utopia becomes possible.” (Brunton 2019, p. 178). As contemporary libertarians “exacerbate the existing crisis” of global warming by pushing deregulation of carbon emissions, the designs of such agorists seem quite alive today. Rumors about imminent hyperinflation or currency collapse are as valuable to Bitcoin HODL-ers (named for a keyboard-smashing typo of a HOLD order) as they are to hucksters of Krugerrands.

By the end of *Digital Cash*, Brunton has little patience for cryptocurrency’s leading success story, Bitcoin: “As of this writing, it seems to have found a role that perfectly exemplifies the present moment: a wildly volatile vehicle for baseless speculation, a roller coaster of ups and downs driven by a mix of hype, price-fixing, bursts of frenzied panic, and the dream of getting rich without doing much of anything” (Brunton 2019, p. 204).

For cultural theorist David Golumbia, by contrast, these developments are unsurprising. Golumbia tends to critique computation as reductionist, all too prone to flatten our experience of education, relationships, and politics into simplistic categories and ersatz quantifications. His 2009 *The Cultural Logic of Computation* chronicled the distortions to human thought and civic association caused by the overreach of digitization (Golumbia 2009). *The Politics of Bitcoin* anticipated an explosion of interest in the troubling adoption of cryptocurrency by white supremacists, criminals, and frauds (Burns 2018; Malik 2018).

Well-versed in both critical theory and the philosophy of language, Golumbia interprets key texts in cryptocurrency advocacy as cyberlibertarian propaganda. In 1997, Langdon Winner diagnosed cyberlibertarianism as a linkage of “ecstatic enthusiasm for electronically mediated forms of living with radical, right-wing libertarian ideas about the proper definition of freedom, social life, economics, and politics” (Winner 1997). Libertarian thought tends to derogate government as the chief enemy of liberty—rather than recognizing, as nearly all other political philosophies do, that government is critical to *assuring* freedom, since anarchy is little more than rule by the strongest.

Insights like these serve, for Golumbia, as an Ariadne’s thread to guide him through remarkably solipsistic, fantastic, or dense texts. *The Politics of Bitcoin* is a first-rate work of what Paul Rabinow and William Sullivan (Rabinow and Sullivan 1988) have called “interpretive social science,” carefully elaborating meaning from a set of contested, murky, or ostensibly contradictory texts. Building on the work of Langdon Winner, Golumbia explains that the core tenet of cyberlibertarianism is the insistence that “governments should not regulate the internet” (Golumbia 2016, p. 5). For Golumbia, the original sin of Bitcoin was its systematic effort to promote itself as a somehow “safer” alternative than independent central banks. This anti-system rhetoric had a long history, including far right groups enraged by the power of the Federal Reserve, the New Deal, and the civil rights movement.

Golumbia traces linkages between anti-state and pro-Bitcoin rhetoric in the thought of cryptocurrency advocates. As he explains early in the work, his purpose is “to show how much of the economic and political thought on which Bitcoin is based emerges directly from ideas that travel the gamut from the sometimes-extreme Chicago School economics of Milton Friedman to the explicit extremism of Federal Reserve conspiracy theorists.” (Golumbia 2016, p. 12). Friedman and his monetarist disciples accommodated themselves to the Federal Reserve (the central bank of the U.S.), but sought to tightly constrain it. Golumbia reviews the origins of their ideas, and then describes their appropriation in the present day.

Like much laissez-faire economic thought, these extreme ideas’ viral success owes much to their simplicity. Some

right-wing theorists of money characterize central banking as a conspiracy where insiders can plot to devalue currency by printing ever more dollars. *Real* value, they insist, can only be measured by something that is scarce because its supply cannot be dramatically altered by human will. Gold fits this bill; paper (or, worse, digital entries on a government balance sheet) does not. The Bitcoin imaginary is rife with stories of inflation sparked by incompetent or greedy banking authorities.

This populist worry about inflation is the mirror image of a critical nineteenth century politicization of money, when insurgent reformers were deeply concerned with the problem of *deflation* (that is, the rising burden of debt, and concurrent economic slowdown, that tends to occur when a unit of currency starts gaining value over time). In the 1880s and 90s, American farmers and small businesses were crushed by debt as the real value of what they owed increased over time (rather than decreasing, as it would during an inflationary period). A rigid gold standard kept the government from pursuing a looser monetary policy, which would have better fit the needs of a growing country. A populist demand to smash the “cross of gold” was frustrated at the time, of course, but later crises led to a suspension of the gold standard and a more accommodative monetary regime. Now, there is enormous populist energy in exactly the opposite direction: Bitcoin reflects and reinforces fears of out-of-control central banks printing money willy-nilly, massively devaluing currency. How did this switch occur?

Of course, events like the German, Zimbabwean, and Venezuelan hyperinflations spurred such worries. Quantitative easing provoked both paranoid and entirely justifiable resentments of connected bankers buying up assets on the cheap with easy government credit. But we must also recognize that cryptocurrency’s romance with deflation has also been stoked by ideological movements, entrepreneurial fantasists, and an increasingly unfair financial regulatory system. As Golumbia explains, “It is a cardinal feature of right-wing financial thought to promote the idea that inflation and deflation are the result of central bank actions, rather than the far more mainstream view that banks take action to manage inflation or deflation in response to external economic pressures.” Bitcoin enthusiasts seize this idea as one more rationale to shift assets out of national currencies, abandoning inevitably political and legal governance of money for the “safety” of code.

The law professor Katharina Pistor’s *The Code of Capital* demonstrates how foolish that aspiration may turn out to be. Pistor is primarily concerned with legal, rather than computational, code. Her long and distinguished research career demonstrates why that prioritization makes sense. Pistor has demonstrated the many ways that law is not merely a constraint on finance, but instead is *constitutive* of financial markets. The vast edifice of currency exchanges, derivatives,

swaps, options, and countless other instruments, rests on a foundation of law—or, to be more precise, the relative power of one party to force another to obey the terms of contracts they have made. Pistor has demonstrated the critical role of law in creating and maintaining durable exchanges of equity and debt. Though law to some extent shapes all markets, in finance it is fundamental—the “products” traded are very little more than legal recognitions of obligations to buy or sell, own or owe.

In earlier work, Pistor has argued that “finance is essentially hybrid between state and markets, public and private” (Pistor 2013). And we can see immediately the enormous problems this social fact poses for cyberlibertarians. They want the state out of the (or at least their) money business; Pistor’s legal theory of finance reminds us of just how revolutionary such a wish is. Nevertheless, she gamely recounts the assumptions of cyberlibertarians, on the way to a more realistic account of how the “coding” of capital—the ability of experts to ensure certain claims to assets and income streams are durable, transferable, and enforceable—may increasingly depend on technological (rather than merely legal) prowess.

As Pistor observes, the egalitarian case for automated finance is a simple one: “When the digital code replaces the legal code,” we are assured, “the commitments we make to one another become hardwired, and even the powerful cannot simply wiggle out of them.” (Pistor 2019, p. 184). However, the problem of the wealthy evading contracts should be counterbalanced against the many ways in which the wealthy use contracts to ruthlessly dun debtors, sidetrack labor disputes into feckless arbitral panels, and reroute assets away from progressive taxation. Digital utopists’ strategic decision to raise the salience of the powerful’s evasion of contractual obligations is a political maneuver. Indeterminacy and lack of enforceability are not always and everywhere problematic features of contracts. Indeed, a key part of legal training is the ability to spot the ways that judicial precedent, legislation, and regulation enable us to escape from bad bargains, or at least mitigate their effects.

Cryptocurrency buffs may cede those points, and then pivot to the economic and political case for digital finance. Automated recordation of assets and transfers is presumed to be cheaper and more egalitarian than an army of clerks and lawyers. But as Pistor patiently reminds us, “Someone has to write the code, watch it, and fix its bugs; and someone must find an answer to the question of whose interests the code serves, or perhaps ought to serve.” (Pistor 2019, p. 185). Rather than the “flat world” of Tom Friedman’s dreams, automated finance just introduces new hierarchies: among cryptocurrencies; within any particular one, among high level coders and those who just do what they are told; and, of course, between the coder class and ordinary users (Pasquale 2019). Indeed, Pistor predicts that large financial institutions will try to coopt the utopian energy that Brunton describes, by

“enclos[ing] the digital code in law and leav[ing] little space to the digital utopists.” (Pistor 2019, p. 186).

Even when domesticated by established financial interests, both blockchain and smart contracts may be of limited value. There are many contractual relationships that are too complex and variable, and require too much human judgment, to be reliably coded into software. Code may reflect and in large part implement what the parties intended, but should not *itself* serve as the contract or business agreement among them.

Moreover, even if immutability of contractual terms were possible, it is not always desirable; when conditions change enough, re-negotiation is a strength of traditional law, not a weakness. So, too, do statutory opt-outs (which let persons break contracts in certain situations, such as an emergency or illness) render legally unenforceable a contract coded to execute no matter what. An immutable ledger distributed across thousands or millions of computers and servers may also directly conflict with common data protection laws: how can a “right to be forgotten” or “right to erasure” operate if the relevant record is not merely ubiquitous, but hard-coded into permanence? Cyberlibertarians may respond that such laws themselves are infringements on sacred rights of free expression, but even they would likely blanch at the prospect of the uncontrollable copying and permanent recording of, say, their breached medical records. So long as hackers menace the security of any computer code, data, and communications, sophisticated and powerful parties are unlikely to opt into a brave new world of totally automated finance.

For the marginalized, though, code may indeed become a law unto itself. To be truly the final word in contracting, smart contracts would need both parties to give up other rights they might have outside the four corners of their coded relationship. Since the *Lochner* era in the United States, a libertarian legal movement has prioritized one goal in commercial life above nearly all others: the right to give up one’s rights. Styled as “freedom of contract,” such a right includes the liberty to sacrifice one’s rights to a receive a minimum wage, days off, or a trial in a court of law when those (or any other) rights are violated. Widely known as “forced arbitration,” that last proviso is an increasingly powerful unraveller of law in the realms of both employment and consumption, all too often consigning legitimate claims to byzantine and biased arbitral fora. If courts allow parties to opt into smart contracts with no appeal to the statutes and regulations that govern the rest of finance, the crypto dream of an alternative legal system may finally be realized—with nightmarish costs for the unwary or unlucky. Imagine a car programmed to shut off the moment a payment is late, and you have a sense of the implications of automated enforcement of loan terms.

Despite the precision and breadth of her critiques of Bitcoin in particular and blockchain technologies generally,

Pistor remains open-minded about future advances in the “digital coding” of finance. The bulk of her book traces the manifest unfairness wrought by centuries of development of trust, bankruptcy, securities, tax, and intellectual property law toward protecting the interests of the wealthy and powerful. From that perspective, *any* alternative to the legal coding of capital may seem promising. However, it is hard to imagine how the utopian visions of cryptocurrency would mesh with more pragmatic reforms of finance law and policy, or with the increasingly evident importance of the state as a final guarantor of value and liquidity. Cryptocurrency enthusiasts cannot escape the legal foundations of finance, no matter how ingeniously they code their next initial coin offering.

The divide between economics and politics seems both obvious, and obviously ideological. There are markets and states. The market is a realm of free exchange; the state keeps order. Price signals nudge consumers and businesses to decide when to buy and sell; command and control bureaucracies allocate resources governmentally. The market’s natural order is spontaneous; the state’s man-made rationality is planned. Societies exist on a continuum between free markets and statist control. These distinctions are not only familiar ideological crutches for an American right prone to paint regulation as the antithesis of freedom. They have also tended to divide up jurisdictional authority in universities, luring researchers of governments to political science departments, and experts in commodification and exchange to economics.

However ideologically or functionally useful these divides may have been in the past, we now know that they obscure just as much as they illuminate (Pasquale 2018). The state can be [entrepreneurial](#); private enterprise can be [predatory and sclerotic](#) (Link and Link 2009). Market logics may have invaded society, but social logics have interpenetrated markets, too. The hottest new methodology in the legal academy is law and political economy (LPE). In a pointed corrective to decades of hegemony by law and economics in so-called “private law fields,” LPE studies critical public interventions that created the markets now so often treated as sanctuaries of free choice and natural order. For example, segregated neighborhoods did not just “happen” in the United States, as the spontaneous result of millions of individual decisions. They were structured by federal home finance policies, by judicial decisions to enforce “restrictive covenants” preventing transfers to African Americans, and numerous other legal factors. Sociologists, historians, and many others can help us trace back the roots of contemporary “free choice” to struggle and coercion.

As methodological lenses proliferate, economists can no longer claim a monopoly of expertise on the economy. Other social science and humanities scholars have vital insights, advancing deep and nuanced accounts of the role of money in society, among many other dimensions of commerce.

Academic study of the economy is now, more than at any time over the past 70 years of creeping specialization, up for grabs. The struggle of futurist fintech to reinvent basic anti-fraud and consumer protection measures shows how deeply financial markets depend on the state to function—and how, nevertheless, powerful actors in finance are using both legal and digital code to reduce the scope and intensity of state power.

They are likely to continue to succeed in doing so, at least for the foreseeable future. Cyberlibertarian ideology is ascendant, evident in the talking points of hard-right Trump appointees and white papers of DC think tanks. Funded by large technology firms, the Kochs, and the many other branches of the neoliberal thought collective that Philip Mirowski (2014) has described, key “blockchain experts” hype cryptocurrency as the first step of a journey into a libertarian future. A formidable coalition of finance lobbyists and nervous oligarchs aid cyberlibertarians by undermining the power of legitimate authorities to shape (or even monitor) global capital flows.

To the extent it signs on to the post-regulatory agenda of futurist fintech, established banks are playing a dangerous game: they need the power of the state to enforce their contracts, and to serve as lender-of-last-resort in case of crisis. Given the temptations of massive returns via excess leverage, they will continue to resist state power, undermining the very mechanisms that are necessary to save capitalism from itself, and weakening the very tax and monetary authorities necessary (in conventional economic theory) to fund the next bailout. This is of course an old story in capitalism: As Andreas Malm described in *Fossil Capital*, and Samuel Stein related in the recent *Capital City*, bosses have always wanted the succor of the state (providing infrastructure, health care, and other necessary subsistence to workers) without paying the taxes so obviously necessary to support it (Malm 2016; Stein 2019). In this environment, expect to see more appeals to the digital as the source of a “free lunch,” a chance to get “something for nothing” via new forms of money and exchange.

Cryptocurrency is alluring now because finance’s present is so alarmingly exploitative and inefficient. But things could always get worse. Both incrementalist and futurist fintech expose the hidden costs of digital efforts to circumvent or co-opt state monetary authorities. They help us overcome the disciplinary divides—between politics and economics, or law and business—that have obscured the stakes of the metaphors and narratives that dominate contemporary conceptions of currency. We face a stark choice: recognize the **public nature of money** and redirect its creation toward public ends, or allow the power of the state to increasingly be annexed to the privateers best poised to stoke public enthusiasm for private monies, and to profit immensely from the uncertainty they create (Pasquale 2019a).

References

- ACLU. (2014). *Metadata: Piecing together a privacy solution*. Available via ACLU of California. Retrieved February 17, 2020, from <https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf>.
- Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless workplace surveillance. *California Law Review*, 105(3), 735–776. <https://doi.org/10.15779/Z38BR8MF94>.
- Angwin, J., Scheiber, S., & Tobin, A. (2017). *Facebook job ads raise concerns about age discrimination*. Available via The New York Times. Retrieved February 17, 2020, from <https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html>.
- Barlyn, S. (2018). *Strap on the Fitbit: John Hancock to sell only interactive life insurance*. Available via Reuters. <https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL>.
- Beedham, M. (2019). *Here’s how to fight back against bitcoin-ransoming malware*. Available via TNW Hard Fork. Retrieved February 17, 2020, from <https://thenextweb.com/hardfork/2019/09/26/heres-how-to-fight-back-against-bitcoin-ransoming-malware-ransomware/>.
- Berlant, L. (2011). *Cruel optimism*. Durham, NC: Duke University Press.
- Blacker, D. J. (2013). *The falling rate of earning and the neoliberal endgame*. Washington, DC: Zero Books.
- Bruckner, M. A. (2018). The promise and perils of algorithmic lenders’ use of big data. *Chicago-Kent Law Review*, 93(1), 3–60.
- Brunton, F. (2019). *Digital cash: The unknown history of the anarchists, utopians, and technologists who created cryptocurrency*. Princeton, NJ: Princeton University Press.
- Burns, J. (2018). *Cut off from big Fintech, white nationalists are using bitcoin to raise funds*. Available via Forbes. Retrieved February 17, 2020, from <https://www.forbes.com/sites/janetwburns/2018/01/03/cut-off-from-big-fintech-white-supremacists-are-using-bitcoin-to-raise-funds/#301d1f9e33b3>.
- Citron, D. K. (2008). Technological due process. *Washington University Law Review*, 85(6), 1249–1313.
- Citi., (2018). Investment themes in 2018: How much longer can the cycle run? Available via <https://www.citivelocity.com/citigps/investment-themes-2018/>. Accessed. 12/15/20.
- Financial Crisis Inquiry Commission (FCIC). (2011). *Final report of the national commission on the causes of the financial and economic crisis in the United States*. Available via govinfo. Retrieved February 18, 2020, from <https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf>.
- Gibbs, S. (2015). *Women less likely to be shown ads for high-paid jobs on Google, study shows*. Available via The Guardian. Retrieved February 18, 2020, from <https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>.
- Golumbia, D. (2009). *The cultural logic of computation*. Cambridge, MA: Harvard University Press.
- Golumbia, D. (2016). *The politics of bitcoin: Software as right-wing extremism*. Minneapolis, MN: University of Minnesota Press.
- Hill, R. P., & Kozup, J. C. (2007). Consumer experiences with predatory lending practices. *The Journal of Consumer Affairs*, 41(1), 29–46. <https://doi.org/10.1111/j.1745-6606.2006.00067.x>.
- Kotsko, A. (2015). *Creepiness*. Washington, DC: Zero Books.
- Leber, J. (2016). *This new kind of credit score is all based on how you use your cell phone*. Available via Fast Company. Retrieved February 18, 2020, from <https://www.fastcompany.com/3058725/this-new-kind-of-credit-score-is-all-based-on-how-you-use-your-cellphone>.
- Lin, T. C. W. (2014). The new financial industry. *Alabama Law Review*, 65(3), 567–623.

- Lin, T. C. W. (2015). Infinite financial intermediation. *Wake Forest Law Review*, 50(3), 643–669.
- Link, A. N., & Link, J. R. (2009). *Government as entrepreneur*. New York: Oxford University Press.
- Malik, N. (2018). *How criminals and terrorists use cryptocurrency: And how to stop it*. Available via Forbes. Retrieved February 18, 2020, from <https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#39df3d983990>.
- Malm, A. (2016). *Fossil capital: The rise of steam power and the roots of global warming*. New York: Verso.
- McGettigan, A. (2013). *The great university gamble: Money, markets and the future of higher education*. London: Pluto Press.
- McMillan Cottom, T. (2018). *Lower ed: The troubling rise of for-profit colleges in the new economy*. New York: The New Press.
- Metz, R. (2018). *This company embeds microchips in its employees, and they love it*. Available via MIT Technology Review. Retrieved February 18, 2020, from <https://www.technologyreview.com/s/611884/this-company-embeds-microchips-in-its-employees-and-they-love-it/>.
- Mierzewski, E., & Chest, J. (2013). Selling consumers not lists: The new world of digital decision-making and the role of the fair credit reporting act. *Suffolk University Law Review*, 46, 845–880.
- Mirowski, P. (2014). *Never let a serious crisis go to waste: How neoliberalism survived the financial meltdown*. New York: Verso Books.
- Newfield, C. (2016). *The great mistake: How we wrecked public universities and how we can fix them*. Baltimore, MD: Johns Hopkins University Press.
- Pasquale, F. (2008). Internet nondiscrimination principles: Commercial ethics for carriers and search engines. *University of Chicago Legal Forum*, 2008(1), 263–299.
- Pasquale, F. (2015). Reforming the law of reputation. *Loyola University Chicago Law Journal*, 47, 515–539.
- Pasquale, F. (2016). Platform neutrality: Enhancing freedom of expression in spheres of private power. *Theoretical Inquiries in Law*, 17(1), 487–513.
- Pasquale, F. (2017). Toward a fourth law of robotics: Preserving attribution, responsibility, and explainability in an algorithmic society. *Ohio State Law Journal*, 78(5), 1243–1255.
- Pasquale, F. (2018). New economic analysis of law: Beyond technocracy and market design. *Critical Analysis of Law*, 5(1), 1–18.
- Pasquale, F. (2019). A rule of persons, not machines: The limits of legal automation. *George Washington Law Review*, 87(1), 1–55.
- Pasquale, F. (2019a). Realities and relationships in public finance. *Provocations*, 2, 21–28. <https://www.provocationsbooks.com/2019/02/05/realities-and-relationships-in-public-finance/>.
- Peppet, S. R. (2015). Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Northwestern University Law Review*, 105(3), 1153–1204.
- Pistor, K. (2013). Law in finance. *Journal of Comparative Economics*, 41(2), 311–314.
- Pistor, K. (2019). *The code of capital: How the law creates wealth and inequality*. Princeton, NJ: Princeton UP.
- Polk, D. (2019). *Time to get serious about microchipping employees and biometric privacy laws*. Available via Law Fuel. Retrieved February 18, 2020, from <http://www.lawfuel.com/blog/time-to-get-serious-about-microchipping-employees-and-biometric-privacy-laws/>.
- Rabinow, P., & Sullivan, W. (Eds.). (1988). *Interpretive social science—A second look*. Berkeley and Los Angeles, CA: University of California Press.
- Sacasas, L. M. (2013). *Borg complex*. Available via The Frailest Thing. Retrieved February 18, 2020, from <https://thefrailestthing.com/2013/03/01/borg-complex-a-primer/>.
- Schiller, R. J. (2019). *Narrative economics: How stories go viral and drive major economic events*. Princeton, NJ: Princeton University Press.
- Scism, L. (2019). *New York insurers can evaluate your social media use—If they can prove it's needed*. Available via The Wall Street Journal. Retrieved February 18, 2020, from <https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social-media-use-if-they-can-prove-why-its-needed-11548856802>.
- Seamster, L., & Charron-Chénier, R. (2017). Predatory inclusion and education debt: Rethinking the racial wealth gap. *Social Currents*, 4(3), 199–207. <https://doi.org/10.1177/2329496516686620>.
- Senior, A. (2018). *John Hancock leaves traditional life insurance model behind to incentivize longer, healthier lives*. Available via CISION PR Newswire. Retrieved February 18, 2020, from <https://www.johnhancock.com/news/insurance/2018/09/john-hancock-leaves-traditional-life-insurance-model-behind-to-incentivize-longer%2D%2Dhealthier-lives.html>.
- Stein, S. (2019). *Capital city: Gentrification and the real estate state*. New York: Verso.
- Taylor, K.-Y. (2019). *Predatory inclusion*. n+1 Magazine 35. Retrieved February 18, 2020, from <https://nplusonemag.com/issue-35/essays/predatory-inclusion/>.
- Tene, O., & Polonetsky, P. (2014). A theory of creep: Technology, privacy, and shifting social norms. *Yale Journal of Law and Technology*, 16(1), 59–102.
- The Guardian Editorial. (2018). *The Guardian view on big data and insurance: Knowing too much*. Available via The Guardian. Retrieved February 18, 2020, from <https://www.theguardian.com/commentisfree/2018/sep/27/the-guardian-view-on-big-data-and-insurance-knowing-too-much>.
- Upturn. (2015). *Online lead generation and payday loans*. Available via Upturn. Retrieved February 18, 2020, from <https://www.upturn.org/reports/2015/led-astray/>.
- Van Dam, A. (2019). *Algorithms were supposed to make Virginia judges fairer: What happened was far more complicated*. Available via The Washington Post. Retrieved February 18, 2020, from <https://www.washingtonpost.com/business/2019/11/19/algorithms-were-supposed-make-virginia-judges-more-fair-what-actually-happened-was-far-more-complicated/>.
- Variyar, M., & Vignesh, J. (2017). *The new lending game, post-demonetisation*. Available via ET Tech. Retrieved February 18, 2020, from <https://tech.economictimes.indiatimes.com/news/technology/the-new-lending-game-post-demonetisation/56367457>.
- Vincent, J. (2015). *Woman fired after disabling work app that tracked her movements 24/7*. Available via The Verge. Retrieved February 18, 2020, from <https://www.theverge.com/2015/5/13/8597081/worker-gps-fired-myra-arias-xora>.
- Warner, M. R. (2019). *Senators introduce bipartisan legislation to ban manipulative 'dark patterns'*. Available via Mark R. Warner: Press releases. Retrieved February 18, 2020, from <https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns>.
- White, R. W., Doraiswamy, P. M., & Horvitz, E. (2018). Detecting neurodegenerative disorders from web search signals. *NPJ Digital Medicine*, 1(8), 1–4. <https://doi.org/10.1038/s41746-018-0016-6>.
- Winner, L. (1997). Cyberlibertarian myths and the prospects for community. *Computers and Society*, 27(3), 14–19. <https://doi.org/10.1145/270858.270864>.
- World Economic Forum. (2017). *Beyond Fintech: A pragmatic assessment of disruptive potential in financial services*. Available via <https://es.weforum.org/reports/beyond-fintech-a-pragmatic-assessment-of-disruptive-potential-in-financial-services>. Accessed 12/15/20.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.